PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-249899**
(43)Date of publication of application : **14.09.2001**

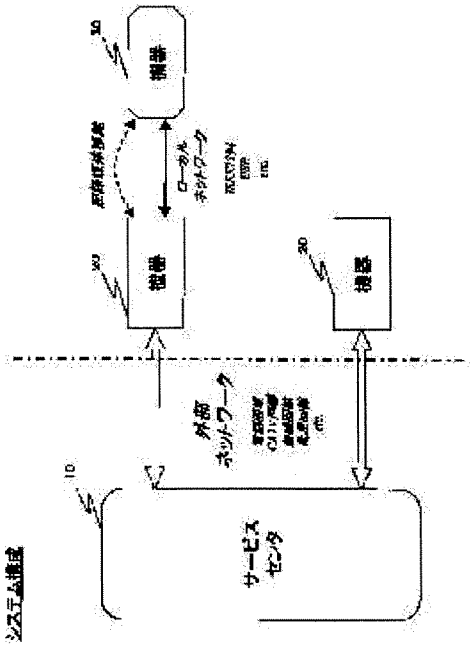
(51)Int.Cl. **G06F 15/00**
G06F 13/00
G06F 17/60
H04Q 7/38
H04L 9/32
H04L 12/66

(21)Application number : **2000-062213**
(22)Date of filing : **07.03.2000**

(71)Applicant : **SONY CORP**
(72)Inventor : **ISHIBASHI YOSHITO**
ASANO TOMOYUKI
OKA MAKOTO

(54) SERVICE PROVIDING SYSTEM VIA COMMUNICATION MEANS, ITS METHOD, SERVICE MEDIATING DEVICE AND PROGRAM PROVIDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a service providing system by which maintenance and control via an external network concerning an electronic unit without having a communication part and a cipher processing part are performed by keeping a communication secret.
SOLUTION: A controlled unit (low-order unit) being the object of maintenance or control, etc., is constituted to transfer data to a high-order unit via a local network or via an information recording medium such as a memory stick. The high-order unit is provided with a communication means to transfer data received from a service center to the controlled unit (low-order unit) via the local network or the information recording medium. In the high-order unit, the safety of communication data is guaranteed since a communication processing is performed with the service center after enciphering data so that important information such as control information or individual information required for providing control information is prevented from being leaked.



LEGAL STATUS

[Date of request for examination] 21.12.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－249899
（P2001－249899A）
(43)公開日　平成13年９月14日(2001.9.14)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ　５Ｂ０４９
			３３０Ｚ　５Ｂ０８５
	３２０		３２０Ａ　５Ｂ０８９
13/00	３５１	13/00	３５１Ｚ　５Ｊ１０４
	３５７		３５７Ａ　５Ｋ０３０

審査請求　未請求　請求項の数26　ＯＬ　（全 85 頁）　最終頁に続く

(21)出願番号　特願2000－62213(P2000－62213)

(22)出願日　平成12年３月７日(2000.3.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

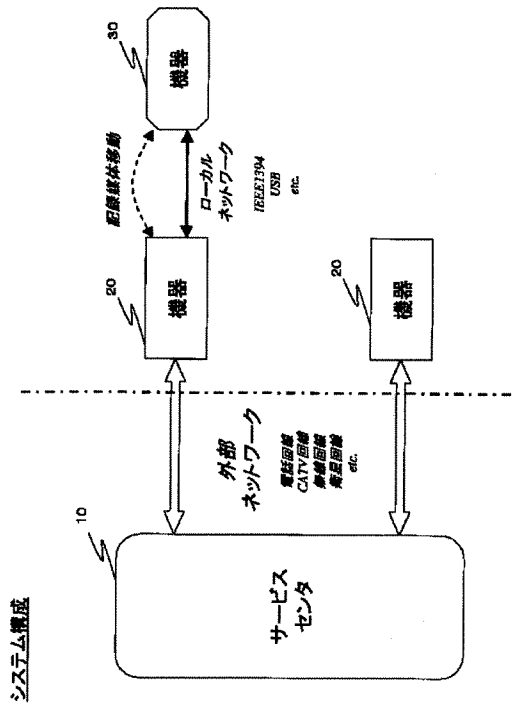
最終頁に続く

(54)【発明の名称】　通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体

(57)【要約】

【課題】　通信部、暗号処理部を持たない電子機器に対する外部ネットワークを介したメンテナンス、制御を通信の秘密を保持して可能とするサービス提供システムを実現する。

【解決手段】　メンテナンス、制御等の対象である制御対象機器（下位機器）を上位機器にローカルネットワークを介して、あるいはメモリスティック等の情報記録媒体を介してデータ転送可能な構成とする。上位機器は通信手段を有し、サービスセンタから受信したデータをローカルネットワークまたは情報記録媒体を介して制御対象機器（下位機器）に転送する。上位機器はデータを暗号化した上でサービスセンタと通信処理を実行するため、通信データの安全性が保証され、制御情報、あるいは制御情報を提供するために必要となる個人情報などの重要な情報の漏洩が防止される。



システム構成

【特許請求の範囲】

【請求項１】ローカルネットワークインタフェース手段、または情報記録媒体インタフェース手段の少なくともいずれかを有する制御対象機器と、

外部ネットワークに対するインタフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインタフェース手段または情報記録媒体インタフェース手段のいずれかを介して前記制御対象機器に対してデータ転送可能な構成を有する上位機器とを有し、

前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンタから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システム。

【請求項２】前記サービスセンタおよび前記上位機器は認証処理手段を有し、前記サービスセンタおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項３】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項４】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体を介したデータ転送は、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項５】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項６】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項７】前記サービスセンタおよび前記上位機器間において送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項８】前記上位機器および前記制御対象機器間において転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項９】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項１０】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、

前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項１１】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、

前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項１２】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、

サービスセンタから、該サービスセンタと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、

前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、

を有することを特徴とするサービス提供方法。

【請求項１３】前記サービスセンタから前記上位機器に対するデータ送信ステップの前に、

前記サービスセンタと前記上位機器間での認証処理を実行する認証処理ステップを有し、

前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。

【請求項１４】前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、

前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、
前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１５】前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、
前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、
前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１６】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１７】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１８】前記サービスセンタまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、
前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１９】前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、
前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２０】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２１】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、
前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２２】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、
前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２３】外部ネットワークに対するインタフェース手段と、
暗号処理を実行する暗号処理手段と、
ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段の少なくともいずれかを有し、
前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置。
【請求項２４】前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする請求項２３に記載のサービス仲介装置。
【請求項２５】前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする請求項２３に記載のサービス仲介装置。
【請求項２６】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、
受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、
を有することを特徴とするとするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。さらに詳細には、各種の電子機

器、例えばテレビやビデオデッキ、エアコン、冷蔵庫、電子レンジなどの各種電子機器に対して、通信ネットワーク等の通信手段を介して各種の制御を実行したり、メンテナンス等のサービスを提供する構成において、個々の機器を小型で低コストの構成とすることを可能とするとともに、サービス提供時の制御情報、メンテナンス情報、課金情報等を十分なセキュリティを確保して転送可能とした通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。

【０００２】

【従来の技術】近年、デジタル技術の発展に伴い、多くの電子機器がマイコン等による制御可能な構成となってきている。また複数のコンピュータを結ぶインターネット等の通信ネットワークにより広い地域をカバーするデジタルネットワークが構築されてきている。電子機器を通信ネットワークに接続することによって、電子機器をネットワークを介して遠隔地から制御したりメンテナンスを行なったり、あるいは電子機器ユーザに対してメンテナンス情報の提供を行なうなど、ネットワークを通じた情報伝達形態が盛んになってきている。

【０００３】具体的には、各種電子機器に対する制御、メンテナンス等のサービスを提供するサービスセンタを設置し、サービスセンタとユーザの電子器間を電話回線、ケーブルテレビ回線、インターネット、無線回線、衛星回線などで接続して各種サービスを提供する構成が実施されている。また、これらのサービス提供システムにおいてユーザ情報、口座情報等の各種決済情報を登録することにより提供したサービスに対して課金処理を行う構成も普及しつつある。

【０００４】

【発明が解決しようとする課題】しかし、このような、電子機器に対するネットワーク等の通信回線を介したサービス提供構成においては、サービス機関とユーザ機器との間をインターネット等の通信手段を介してデータをそのまま送受信することが多いため、例えば個人的な情報が漏洩したり改竄される可能性がある。たとえば、サービス料金に対する課金のためのユーザの銀行口座やクレジットカード番号などの情報は、不正に扱われると重大な被害をもたらす場合があり、インターネットのように複数のユーザが同じ回線を共有するモデルにおいての個人情報を含むデータの送受信は、情報の保護の観点から問題がある。

【０００５】また、現在の通信手段を介したサービス提供システムでは、ネットワーク等を介したサービスを受けるために、サービスを受けるすべての機器がサービスセンタと外部ネットワーク等を経由して直接接続できる構成を持つ必要があった。すなわち、サービス通信手段としてのモデム、インタフェース等がユーザの機器に備わっていることが必要とされている。しかし、このようなサービスを受けるためにすべての機器に通信のためのモジュールを備えることは、コスト面、機器の小型化の点からも好ましいものではない。特に小型化が重要となる機器においてはこの問題は顕著となる。さらに同様の理由で、すべての機器に高度なセキュリティ機能モジュールを構成することも現実的ではなく、これらの問題点がネットワークを介するサービス提供システムの普及を阻む要因の１つとなっている。

【０００６】本発明は、上述の問題点、すなわちサービスを受ける電子機器すべてに通信のためのモジュールを備えることを不要とし、また、機器に高度なセキュリティ機能モジュールを構成する必要性をなくすことを可能としたデータ通信システムおよびデータ通信方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の第１の側面は、ローカルネットワークインタフェース手段、または情報記録媒体インタフェース手段の少なくともいずれかを有する制御対象機器と、外部ネットワークに対するインタフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインタフェース手段または情報記録媒体インタフェース手段のいずれかを介して前記制御対象機器に対してデータ転送可能な構成を有する上位機器とを有し、前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンタから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システムにある。

【０００８】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器は認証処理手段を有し、前記サービスセンタおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【０００９】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【００１０】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体を介したデータ転送は、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【００１１】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする。

【００１２】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする。

【００１３】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器間において送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【００１４】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器間において転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【００１５】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする。

【００１６】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする。

【００１７】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【００１８】さらに、本発明の第２の側面は、制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、サービスセンタから、該サービスセンタと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするサービス提供方法にある。

【００１９】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタから前記上位機器に対するデータ送信ステップの前に、前記サービスセンタと前記上位機器間での認証処理を実行する認証処理ステップを有し、前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２０】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２１】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２２】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする。

【００２３】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする。

【００２４】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ

有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【００２５】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【００２６】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする。

【００２７】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする。

【００２８】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【００２９】さらに、本発明の第３の側面は、外部ネットワークに対するインタフェース手段と、暗号処理を実行する暗号処理手段と、ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段の少なくともいずれかを有し、前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置にある。

【００３０】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする。

【００３１】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする。

【００３２】さらに、本発明の第４の側面は、制御対象機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするとするプログラム提供媒体にある。

【００３３】本発明の第４の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３４】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３５】

【作用】本発明の機器およびサービスセンタは相互に認証処理を実行し、通信相手の確認を実行するとともに、送信データの暗号化を行っているため、安全なデータ送受信が可能となる。さらに外部ネットワークに対する通信手段を持たず、サービスセンタに直接接続できない機器も、外部ネットワークと直接接続できる上位機器を介してサービスセンタとの通信を安全に行うことができる。

【００３６】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３７】

【発明の実施の形態】［システム概要］図1は本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置の概要を説明するブロック図である。本発明のシステムはユーザ機器に対するサービスを提供するサービスセンタ１０、サービスセンタ１０とのデータ送受信を実行するサービス仲介装置としての上位機器２０、上位機器２０を経由して、サービスセンタ１０からの制御等を受ける制御対象機器（下位機器）３０、サービスセンタ１０と上位機器２０とを結ぶ

電話回線、ＣＡＴＶ回線、衛星、無線、インターネット等の外部ネットワーク通信手段、上位機器２０と制御対象機器（下位機器）３０との間を結ぶ、例えば、ＩＥＥＥ１３９４、ＵＳＢ等の通信インタフェースによって通信可能なローカルネットワークからなる。なお、上位機器２０自体がサービスセンタ１０からの制御、メンテナンス等を受ける制御対象機器となることも可能であり、図１の下側に示す上位機器２０は、この態様を示している。

【００３８】図１に示した各構成要素について説明する。本発明のユーザ側の機器は上位機器２０と制御対象機器（下位機器）３０の２種類に大きく分けられる。以下、各機器およびサービスセンタの構成について説明する。

【００３９】＜上位機器＞サービス仲介装置としての上位機器２０は、サービスセンタ１０と電話回線を介した通信が可能なモデム、あるいは、ＣＡＴＶ回線、衛星、その他の無線回線等を介したデータ送受信が可能な通信手段を有する機器である。また、図１の上部に示すように、制御対象機器（下位機器）３０に対して、サービスセンタ１０からのデータを転送したり、制御対象機器（下位機器）３０からサービスセンタ１０への送信データを転送するための手段を有する。

【００４０】図２に上位機器２０の構成を示す。上位機器２０は、サービスを受ける制御対象機器３０との接続用ローカルネットワークを構成するために用いられるＩＥＥＥ１３９４(アメリカ電気電子学会による接続規格)やＵＳＢ(Universal SerialBus)等のインターフェース部としてのローカルインタフェース２０８を備え、他の機器とのデータ通信が可能である。上位機器２０とサービスセンタ１０との通信は電話回線、ケーブルテレビ回線、無線回線、衛星回線、インターネット接続などによって実行される構成とすればよく、これら各通信方法に従った外部インタフェース２０６を持つ。

【００４１】上位機器２０は暗号化・認証や通信の制御を行う専用のＩＣとしての暗号化通信ＩＣ２０５を備える。この暗号化通信ＩＣ２０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、ＩＣには上位機器２０固有の識別子（機器ＩＤ）を格納する記憶手段を備えており、機器の認証の際にこのＩＤを利用する。暗号化・認証通信ＩＣ２０５は、外部からＩＤの書き換え等ができないようにＳＡＭ(Secure Application Module) として構成されることが好ましい。

【００４２】暗号化通信ＩＣ２０５内に格納される機器ＩＤはサービスセンタ１０が発行し、サービスセンタのデータベースには発行済みのＩＤが登録される。なお、セキュリティを高めるために機器ＩＤに、例えば検証ビットを付加する等、冗長性を持たせたデータ構成とすることにより、サービスセンタ１０によるサービス実施時に機器ＩＤの検証ビットを用いた検証を実行するような構成としてもよい。このような構成とすることにより、サービスセンタ１０の発行した正規なＩＤ以外の不正なＩＤを持つ機器をサービス対象から排除することが可能となる。

【００４３】公開鍵暗号方式を利用する上で必要となる、上位機器２０自身の公開鍵と秘密鍵の組およびその公開鍵に対応する公開鍵証明書は予め機器の暗号化通信ＩＣ２０５の記憶部に記録されている。公開鍵証明書は信頼できる証明書発行機関、いわゆる認証局（ＣＡ：Certificate Authority）が発行したものである。

【００４４】本発明の通信手段を介したサービス提供システムにおいては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとる。データ転送の際のセキュリティ構成を実現する１つの手法が、転送データの暗号化処理である。

【００４５】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データに戻すことができる。暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、代表的な例としては暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と、暗号化、復号化に異なる鍵を用いる公開鍵暗号方式とがある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。

【００４６】暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、ディジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解する処理の困難さを利用している。

【００４７】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送

付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステムである。

【００４８】公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【００４９】公開鍵証明書は、証明書のバージョン番号、認証局（ＩＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【００５０】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵等の全体データに対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００５１】認証局は、公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）等の処理を行う。

【００５２】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。本発明の図２に示す上位機器２０では、認証局の公開鍵は暗号化通信ＩＣ２０５の内部メモリに格納されている。

【００５３】なお、上位機器の公開鍵、秘密鍵は、サービスセンタ１０に対して機器登録を実行する際に新たに上位機器が生成、あるいはサービスセンタが生成してこれを受信して上位機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。

【００５４】また、上位機器２０は、複数の鍵の組が格納可能であり、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することができる。上位機器２０には、様々な下位機器としての制御対象機器３０がローカル接続可能であり、例えば制御対象機器３０がＡメーカーのテレビであれば、Ａメーカのサービスセンタ接続用の鍵を用い、制御対象機器３０がＢメーカーのエアコンであれば、Ｂメーカのサービスセンタ接続用の鍵を用いる等の構成が可能となる。

【００５５】上位機器２０は、さらに、暗号化通信ＩＣ２０５の処理制御、各インタフェースを介した通信制御、記憶装置２１０のデータアクセス制御等の各種処理を制御するためのＣＰＵ２０１、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成されるメモリ２０２、機器を操作するユーザに対する指示データ等の表示を行なう表示部２０３、ユーザによる通信開始等の指示を可能とする操作部２０９、ハードディスク、ＣＤ、ＤＶＤ等によって構成される記憶装置２１０を備える。

【００５６】さらに上位機器２０は、機器本来の機能を提供する機器固有部２０４を有する。機器固有部２０４は、機器がたとえばビデオデッキであれば受信データの処理回路や変復調回路、あるいは磁気ドラムやテープ駆動部等であり、例えば電子レンジ等であれば、電子レンジの処理機能を含む。さらに上位機器２０は、メモリースティック、ＦＤ、ＣＤ、ＤＶＤのような情報記録媒体２１１にデータを記録するように構成してもよい。その場合、情報記録媒体２１１とのインターフェース２０７を備える。

【００５７】＜制御対象機器（下位機器）＞制御対象機器（下位機器）３０は、外部ネットワークとの直接接続手段を持たない機器であり、上位機器２０にローカルネットワークを介して接続され、サービスセンタ１０からの制御、メンテナンス等各種サービスを受ける機器である。

【００５８】図３、図４に制御対象機器（下位機器）３０の２つの構成例を示す。図３は、制御対象機器（下位機器）３０が、上位機器と接続するためのローカルネットワークインターフェース３０７を有する構成であり、このローカルネットワークインターフェース３０７を介して上位機器２０と接続され、上位機器２０を介して受領するサービスセンタ１０の制御を受ける。この態様をオンライン型下位機器と呼ぶ。

【００５９】一方、図４に示す制御対象機器（下位機器）３０は、上位機器と接続するためのローカルネットワークインターフェースを持たない構成であり、メモリカード、ＣＤ、ＦＤ等の情報記録媒体３１０に格納された制御情報、メンテナンス情報に基づいて制御を受ける。サービスセンタ１０から受信した制御情報を前述の図２の上位機器の情報記録媒体２１１に格納し、これを制御対象機器（下位機器）３０に取り付けることによってサービスセンタ１０からの制御をオフライン制御として実行することを可能としたものである。

【００６０】制御対象機器（下位機器）３０の構成について説明する。図３のオンライン型の場合、サービスを受ける制御対象機器（下位機器）３０は、上位機器２０との接続用ローカルネットワークを構成するためＩＥＥＥ１３９４やＵＳＢ(Universal Serial Bus)等のインタ

ーフェース部としてのローカルインタフェース３０７を備え、上位機器２０とのデータ通信が可能である。

【００６１】制御対象機器（下位機器）３０は暗号化・認証や通信の制御を行う専用のＩＣとしての暗号化通信ＩＣ３０５を備える。この暗号化通信ＩＣ３０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、暗号化通信ＩＣ３０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。ただし公開鍵暗号方式を利用するためには高い演算能力が必要であることから、資源に制約のある機器においては共通鍵暗号方式のみを利用可能とする構成としてもよい。

【００６２】公開鍵暗号方式を利用する上で必要となる、公開鍵と秘密鍵の組およびその公開鍵に対応する公開鍵証明書は予め制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに記録されている。公開鍵証明書は上述した上位機器２０の場合と同様、信頼できる証明書発行機関、いわゆる認証局（ＣＡ：Certificate Authority）が発行したものである。なお、制御対象機器（下位機器）３０の公開鍵、秘密鍵は、サービスセンタ１０に対して機器登録を実行する際に新たに生成、あるいはサービスセンタが生成してこれを受信して機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。また、制御対象機器（下位機器）３０は、複数の鍵の組を格納可能とした構成としてもよく、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することを可能とした構成としてもよい。なお、サービスセンタ１０の公開鍵は予め機器の暗号化通信ＩＣ３０５の内部メモリに記録されている。なお、共通鍵暗号方式のみを利用する構成とする場合には、共通鍵はサービスセンタ１０によって発行され、制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納する。なお、共通鍵は制御対象機器（下位機器）３０の識別子（ＩＤ）に対応してサービスセンタが保持してもよい。

【００６３】制御対象機器（下位機器）３０は、さらに、暗号化通信ＩＣ３０５の処理制御、各インタフェースを介した通信制御、記憶装置３０９のデータアクセス制御等の各種処理を制御するためのＣＰＵ３０１、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成されるメモリ３０２、機器を操作するユーザに対する指示データ等の表示を行なう表示部３０３、ユーザによる通信開始等の指示を可能とする操作部３０８、ハードディスク、ＣＤ、ＤＶＤ等によって構成される記憶装置３０９を備える。

【００６４】さらに制御対象機器（下位機器）３０は、機器本来の機能を提供する機器固有部３０４を有する。さらに制御対象機器（下位機器）３０は、メモリースティック、ＦＤ、ＣＤ、ＤＶＤのような情報記録媒体３１０にデータを記録するように構成してもよい。その場合、情報記録媒体３１０とのインターフェース３０６を備える。図４のオフライン型の場合、この情報記録媒体３１０を介してサービスセンタ１０からの制御情報を受領する。図３のオンライン型構成では、ローカルネットワークを介するか、あるいは情報記録媒体３１０を介するか、いずれの方法も可能となる。

【００６５】すなわち、図３のオンライン型では、制御対象機器（下位機器）３０はサービスを受ける際、ローカルネットワークインターフェース３０７を用いて上位機器２０に接続し、上位機器２０の外部インタフェース２０６の接続能力を利用してサービスセンタ１０と接続する。このとき通信制御は制御対象機器（下位機器）３０が独自に行う。また、図４のオフライン型では、上位機器２０が制御対象機器（下位機器）３０の代理としてセンタに接続してデータを送受信し、制御対象機器（下位機器）３０はそのデータを上位機器２０で情報記録媒体に記録し、その情報記録媒体を制御対象機器（下位機器）３０に移動し、制御対象機器（下位機器）３０はその情報記録媒体からデータを読み出す。

【００６６】なお、上述した図３のオンライン型、図４のオフライン型の制御対象機器（下位機器）３０は、暗号化通信ＩＣ３０５を有しており、暗号化処理の可能な構成として説明したが、下位機器においては暗号化を行なわず通信を制御するＩＣだけを備えた構成としてもよく、この場合は通信回線を介してオンライン接続、または記憶媒体を介してオフライン接続した上位機器が通信内容の暗号化処理を代行することが可能である。この場合の制御対象機器（下位機器）３０と上位機器２０との認証には機器識別子（ＩＤ）による認証を実行する。

【００６７】＜サービスセンタ＞サービスセンタ１０の構成例を図５に示す。サービスセンタ１０は、外部ネットワークインタフェース１０５および暗号化通信ＩＣ１０４、サービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７、ＣＰＵ１０１、メモリ１０２、さらにこれらを接続するデータバスで構成される。

【００６８】暗号化通信ＩＣ１０４は上位機器２０との通信およびデータの暗号化、サービス提供対象機器の認証などの処理を行う。この暗号化通信ＩＣ１０４にはサービスセンタ固有のセンタ識別子（ＩＤ）が記録されており、これは通信相手となる各機器との相互認証の際に利用する。

【００６９】サービスセンタ１０の暗号化通信ＩＣ１０４は公開鍵暗号方式および共通鍵暗号方式を利用するために必要な演算が可能である。機器情報データベース１０６には、通信対象、たまはサービス対象各機器の識別子（ＩＤ）や公開鍵などの情報が格納されている。データ通信において共通鍵暗号方式を利用する機器の場合には、あらかじめ機器ＩＤとそれに対応する共通鍵をこの機器情報データベース１０６に格納しておく。

【００７０】利用者情報データベース１０７には、サービスセンタ１０からのサービスの提供を受ける機器を管理し、サービスの対価等の支払処理を行なうユーザ、すなわちサービス利用者の識別子（ＩＤ）や各利用者の決済情報などが格納されている。サービス提供用データベース１０３には、サービスを提供するために必要なデータが格納されている。ＣＰＵ１０１は、暗号化通信ＩＣ１０４の処理制御、各インタフェースを介した通信制御、各記憶装置のデータアクセス制御等の各種処理を制御を行ない、メモリ１０２は、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成される。

【００７１】［暗号化・認証レベル］本発明の通信手段を介したサービス提供システムにおいて用いられる公開鍵暗号方式としてはＲＳＡ等、また共通鍵暗号方式としてはＤＥＳ等の暗号方式を用いることが可能であり、必要な強度等を勘案して適切な方式を用いて良い。

【００７２】図6は本発明におけるサービスセンタ１０と上位機器２０、制御対象機器（下位機器）３０との間の接続形態と暗号化・認証レベルをまとめたものである。

【００７３】サービスセンタ１０と上位機器２０とは外部ネットワークで接続されている。また暗号化・認証は公開鍵暗号方式を利用する。上位機器２０と制御対象機器（下位機器）３０との接続の形態には6種類ある。すなわち、（１）制御対象機器（下位機器）３０がローカルネットワークに接続可能で公開鍵暗号方式が利用できる場合、（２）制御対象機器（下位機器）３０がローカルネットワークに接続可能で共通鍵暗号方式のみが利用できる場合、（３）制御対象機器（下位機器）３０がローカルネットワークに接続可能で暗号が利用できない場合、（４）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で公開鍵暗号方式が利用できる場合、（５）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で共通鍵暗号方式のみが利用できる場合、（６）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で暗号が利用できない場合である。なお、一台の上位機器には複数の下位機器を接続可能であり、上位機器２０は、複数の暗号方式に対応可能な構成とすることにより、様々なタイプの制御対象機器（下位機器）との通信が可能となる。なお、制御対象機器（下位機器）の機器ＩＤを参照することにより、上位機器は配下の下位機器を識別可能である。

【００７４】［全体フロー］本発明の通信手段を介したサービス提供システムにおける上位機器２０および制御対象機器（下位機器）３０のサービスセンタ１０を利用した遠隔サービスの提供処理について、以下説明する。

【００７５】図７から図１０までの図はサービス開始から終了に至るまでの全体の処理の流れを簡潔に示したフロー図である。これらのフロー中に含まれる処理の詳細については、後段で説明する。まず、図７～１０を用いて本発明のサービス提供システムの処理の流れの概要を説明する。

【００７６】まず、図７のフローに示すように、上位機器２０をネットワークを介してサービスセンタ１０に対して初めて接続する場合には、ステップＳ７０１に示すサービスセンタ１０への機器登録を行う。初接続時の処理が終了している場合、もしくは機器登録が不要な処理、例えばフリーメンテナンス提供等の場合には、ステップＳ７０２に示す機器認証のステップに移る。機器認証処理フローを図７に示す。これは上位機器２０およびサービスセンタ１０が相互に通信相手の正当性を確認する手続きである。図に示す機器登録プロトコル、機器認証プロトコルについては後段で詳細に説明する。

【００７７】図７に示す、認証プロトコルを実行することにより、不正な機器がサービスを受けたり、サービスセンタ１０と誤って通信を行うことを防ぐことができる。ステップＳ７０２の機器認証に失敗した場合には、エラー処理を行った後、処理を中止する。機器認証に成功した場合は、必要ならば利用者登録を行う。

【００７８】図８に示す利用者登録手続きでは、サービスセンタ１０の利用者情報データベース（図５に示す１０７）に、機器の利用者情報、例えば氏名、サービス料金決済用のクレジットカード番号、あるいは銀行口座番号等の必要情報を登録（ステップＳ８０１）する。その後パスワード等の利用者認証に必要な情報登録（ステップＳ８０２）も行う。

【００７９】図９は、上段が利用者情報、例えば氏名、クレジット番号等の利用者情報変更手続きを示す処理であり、下段が、パスワード等の利用者認証に必要な情報の変更手続きを示すフローである。利用者情報変更手続きでは最初に利用者認証（ステップＳ９０１）を行う。これは正当な利用者以外の者が不正に他人の利用者情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者情報登録（ステップＳ９０２）を行う。

【００８０】利用者情報の登録が完了すると、必要な場合に限り利用者認証に必要な情報、例えばパスワードの利用者認証情報変更手続きを行う。利用者認証情報変更手続きでは、最初に利用者認証を行う。これは正当な利用者以外の者が不正に他人のパスワード等の利用者認証情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者認証情報の変更（ステップＳ９０３）を行う。以上の手続きが終了し、サービスを実施する場合にはサービス実施手続きを行う。

【００８１】図１０に制御対象機器の制御、メンテナン

ス等のサービスの実行処理、すなわちサービス実施手続きフローを示す。サービス実施手続きでは、必要であれば最初に利用者認証を行う。これは正当な利用者以外の者が不正にサービスを受けることを防ぐためである。利用者認証を行うかどうかは、サービスによって異なる。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いてサービスを行う。サービスが完了した後、接続を終了しない場合は機器認証終了時以降の手続きを再度行う。

【００８２】［各プロトコルについて］

（１）機器登録プロトコル

ａ．上位機器

まず、上位機器２０をサービスセンタ１０に対して登録するプロトコルについて説明する。このプロトコルは機器ＩＤ、機種名、機器公開鍵をセンタの機器情報データベースに登録するためのプロトコルである。

【００８３】先の図６で説明したように上位機器２０とサービスセンタ１０との間では、公開鍵暗号方式によって相互認証、データ通信が実行される。公開鍵暗号方式を利用する上で必要となる、上位機器自身の公開鍵と秘密鍵の組があらかじめ上位機器２０の暗号化通信ＩＣ２０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ２０５の内部メモリにあらかじめ格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１１に示し、鍵を生成する場合のプロトコルを図１２に示す。

【００８４】図１１、図１２の処理について説明する。機器登録を行う場合、上位機器２０はサービスセンタ１０に機器登録開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを機器に通知する。同時にサービスセンタ１０は自身のセンタ識別子（ＩＤ）を送信する。

【００８５】上位機器２０はサービスセンタ１０から送られてきたサービスセンタ識別子（ＩＤ）によりセンタを確認し、サービスセンタ１０に自身の上位機器識別子（ＩＤ）、機種名および公開鍵証明書を送信する。上位機器２０の暗号化通信ＩＣ２０５にはサービスセンタ１０の公開鍵が格納されており、サービスセンタ１０への送信の際にはこの公開鍵を用いて送信データを暗号化する。

【００８６】なお、図１２に示す例のように、上位機器２０自身が鍵の組を生成する場合には公開鍵証明書のかわりに上位機器２０が生成した公開鍵をセンタに送信する。

【００８７】上位機器２０からサービスセンタ１０への送信データは、サービスセンタ１０の公開鍵で暗号化されているので、送信データに含まれる上位機器識別子（ＩＤ）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【００８８】上位機器識別子（ＩＤ）等のデータを受信したセンタは、サービスセンタ１０自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の上位機器識別子（ＩＤ）の検証を行い、正当な識別子（ＩＤ）であれば、送信データ中の上位機器識別子（ＩＤ）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。

【００８９】ｂ．制御対象機器（下位機器）

次に、制御対象機器（下位機器）３０をサービスセンタ１０に対して登録するプロトコルについて説明する。

【００９０】制御対象機器（下位機器）３０が機器登録を行う場合には、オンライン型下位機器とオフライン型下位機器で手順が異なる。さらに公開鍵暗号方式が利用できる機器とできない機器とでも異なる。なお、制御対象機器（下位機器）３０が接続する上位機器２０は、この手続きを行う前に上位機器２０とサービスセンタ１０間での機器認証プロトコルを実施しており、センタとの間で認証がなされているものとする。

【００９１】ｂ－１．公開鍵暗号方式のオンライン型下位機器

最初にオンライン型下位機器を用いる場合の手順について図１３に示す。オンライン型下位機器で公開鍵が利用できる場合、公開鍵暗号方式を利用する上で必要となる、制御対象機器（下位機器）３０自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ３０５の内部メモリに格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１３に示し、鍵を生成する場合のプロトコルを図１４に示す。

【００９２】図１３、図１４の処理について説明する。機器登録を行う場合、最初に制御対象機器（下位機器）３０は上位機器２０に対して機器登録開始要求を発行する。これを受け取った上位機器２０はサービスセンタ１０に機器登録開始要求を中継する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。そして上位機器２０は機器登録開始が可能であることを制御対象機器（下位機器）３０に対して通知する。

【００９３】この機器登録開始確認通知を受け取ると、制御対象機器（下位機器）３０は制御対象機器（下位機

器）自身の機器ＩＤ、機種名、公開鍵証明書をセンタの公開鍵で暗号化し、上位機器に送信する。なお、図１４に示すように下位機器が鍵の組を生成する場合には、公開鍵証明書の代わりに自身の公開鍵を上位機器２０に送信する。これを受け取った上位機器２０は、これらの受信データをそのままサービスセンタに中継する。

【００９４】制御対象機器（下位機器）３０から上位機器２０、サービスセンタ１０へ送信されるデータは、サービスセンタ１０の公開鍵で暗号化されているので、送信データに含まれる制御対象機器（下位機器）識別子（ＩＤ）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【００９５】制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、サービスセンタ１０自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当な識別子（ＩＤ）であれば、送信データ中の制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。

【００９６】上位機器２０はサービスセンタ１０から受信した処理完了通知もしくはエラー通知を制御対象機器（下位機器）３０に中継する。

【００９７】ｂ－２．共通鍵暗号方式のオンライン型下位機器

公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオンライン型下位機器の機器登録手順について述べる。

【００９８】この場合のプロトコルを図１５に示す。この場合も、上位機器２０は機器登録開始が可能であることを制御対象機器（下位機器）３０に対して通知するまでの処理は同一である。制御対象機器（下位機器）３０が機器登録開始確認通知を受け取ると、制御対象機器（下位機器）３０は自身の機器ＩＤ、機種名を上位機器２０に送信する。

【００９９】この場合、上位機器２０に送信される機器ＩＤ、機種名情報は暗号化されていないが、ローカルネットワーク上であるので外部ネットワークに比べてセキュリティ上の問題は比較的少ないと考えられる。上位機器２０は制御対象機器（下位機器）３０から受け取った情報をサービスセンタ１０の公開鍵で暗号化する。すなわち、上位機器２０がデータの暗号化を代行する。この後の処理は公開鍵暗号方式が利用できる下位機器の場合の手順と同一であるので説明を省略する。

【０１００】ｂ－３．公開鍵暗号方式のオフライン型下位機器

続いてオフライン型下位機器における機器登録手順について述べる。オフライン型下位機器で公開鍵暗号方式が利用できる場合、公開鍵暗号方式を利用する上で必要となる、制御対象機器（下位機器）３０自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ３０５の内部メモリに格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１６に示し、鍵を生成する場合のプロトコルを図１７に示す。

【０１０１】図１６、図１７の処理について説明する。制御対象機器（下位機器）３０は最初に情報記録媒体を認証する。情報記録媒体３１０は例えばメモリカードであり、メモリカードの識別子等を用いた認証処理が実行される。認証が成立すると、制御対象機器（下位機器）３０は自身の制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書（図１６）もしくは公開鍵（図１７）をサービスセンタの公開鍵で暗号化し、情報記録媒体３１０に転送する。

【０１０２】データ転送が完了した後、情報記録媒体３１０を制御対象機器（下位機器）３０下位機器から取り外し、上位機器２０に装着する。上位機器２０は情報記録媒体２１１（情報記録媒体３１０と同じ）が装着されると、情報記録媒体の認証を開始する。情報記録媒体認証が終了した後、上位機器２０は情報記録媒体からデータを転送（読み出し処理）する。転送終了後、上位機器２０はサービスセンタ１０に機器登録開始要求を制御対象機器（下位機器）３０の代理として行う。

【０１０３】サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。そして上位機器２０は情報記録媒体２１１から転送したデータをそのままセンタに送信する。情報記録媒体２１１から読み出された制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、自身の秘密鍵で上位機器２０が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当なＩＤであれば、受信した制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書（図１６）もしくは公開鍵（図１７）を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に処理完了通知を返す。データの復号あるいは制御対象機器（下位機器）識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。上位機器２０は情報記録媒体２１１に処理完了通知もしくはエラー通知を転送する。その

後、情報記録媒体２１１を上位機器２０から制御対象機器（下位機器）３０に移動する。制御対象機器（下位機器）３０は情報記録媒体認証を行った後、サービスセンタ１０からの通知を情報記録媒体から転送する。通知内容がエラー通知であれば、再度機器登録を試みる。

【０１０４】ｂ－４．共通鍵暗号方式のオフライン型下位機器

公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオフライン型下位機器の機器登録手順について述べる。この場合のプロトコルを図１８に示す。制御対象機器（下位機器）３０は最初に情報記録媒体３１０を認証する。その後、制御対象機器（下位機器）３０は自身の機器ＩＤ、機種名を情報記録媒体３１０に転送する。転送が完了した後、情報記録媒体３１０を制御対象機器（下位機器）３０から取り外し、上位機器２０に装着する。

【０１０５】上位機器２０は情報記録媒体２１１（＝情報記録媒体３１０）が装着されると、情報記録媒体２１１の認証を開始する。情報記録媒体２１１の認証が終了した後、上位機器２０は情報記録媒体２１１からデータを転送する。転送終了後、上位機器２０はサービスセンタ１０に機器登録開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。上位機器２０は情報記録媒体２１１から転送したデータをサービスセンタ１０の公開鍵で暗号化し、センタに送信する。情報記録媒体２１１から読み出された制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、自身の秘密鍵で上位機器２０が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当なＩＤであれば、受信した制御対象機器（下位機器）識別子（ＩＤ）、機種名を機器情報データベース１０６に登録する。その後の処理完了通知などの処理は、公開鍵暗号方式が利用できるオフライン型下位機器を用いる場合と同様である。

【０１０６】［機器認証プロトコル］次に、サービスセンタ１０、上位機器２０、制御対象機器（下位機器）３０の相互において実行される機器認証プロトコルの詳細について説明する。機器認証プロトコルは、データ通信を行なう２者間で通信相手の正当性を確認するために実行されるプロセスである。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。以下、上位機器２０を中心として行われる機器認証プロトコルと、制御対象機器（下位機器）３０を中心として行われる機器認証プロトコルについて、それぞれ説明する。

【０１０７】ａ．上位機器

まず、上位機器２０とサービスセンタ１０との間で実行される互いの正当性を確認する機器認証プロトコルについて説明する。

【０１０８】図１９にサービスセンタ１０と上位機器２０とが機器認証を行う場合のプロトコルを示す。まず上位機器２０はサービスセンタ１０に機器認証開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを機器に通知する。この際、サービスセンタ１０は自身のセンタＩＤを送信する。

【０１０９】上位機器２０はサービスセンタ１０から、認証開始可能の応答を受領すると、上位機器２０自身の機器ＩＤを送信する。その後、サービスセンタ１０と上位機器２０との間で相互認証を行う。相互認証の手続きとしては、たとえばＩＳＯ９７９８に示されている手続きを利用することができる。

【０１１０】ＩＳＯ９７９８の相互認証手続きとして、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図２０を用いて説明する。図２０において、公開鍵暗号方式としてＥＣＣを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図２０において、Ａ、Ｂの一方がサービスセンタ１０、他方が上位機器２０に相当する。

【０１１１】まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。

【０１１２】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書認証局（ＣＡ）の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出す。

【０１１３】Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【０１１４】次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（X座標とY座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵

証明書とともにＡに返送する。

【０１１５】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１１６】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１１７】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１１８】このような相互認証処理において生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行することにより、第三者に対する通信データの漏洩が防止される。なお、データの暗号化に必要なセッション鍵の生成はサービスセンタ１０、上位機器２０のどちらが行ってもよい。相互認証やセッション鍵の交換が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、センタは上位機器に処理完了を通知する。

【０１１９】ｂ－１．オンライン型下位機器

次にサービスセンタ１０とオンライン型の制御対象機器（下位機器）３０とが機器認証を行う場合について述べる。この場合のプロトコルを図２１に示す。

【０１２０】まずオンライン型の制御対象機器（下位機器）３０は上位機器２０に機器認証開始要求を送信する。上位機器２０は要求に応えられる状態であれば、機器認証開始可能であることを制御対象機器（下位機器）３０に通知する。制御対象機器（下位機器）３０は上位機器２０に自身の機器ＩＤを送信する。そして上位機器２０と制御対象機器（下位機器）３０との間で相互認証を行う。

【０１２１】なお、上位機器２０と制御対象機器（下位機器）３０との間での相互認証は、前述のサービスセンタ１０と上位機器２０との間の相互認証処理として説明した図２０の公開鍵暗号方式の認証処理として行なってもよいし、共通鍵暗号方式による相互認証を行なってもよい。

【０１２２】共通鍵暗号方式を用いた相互認証方法を、図２２を用いて説明する。図２２は共通鍵暗号方式としてＤＥＳを用いた例であるが、同様な共通鍵暗号方式であればその他の方法も適用可能である。図２２において、Ａ、Ｂのいずれかが上位機器２０、他方が制御対象機器（下位機器）３０に対応する。

【０１２３】まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。

【０１２４】これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１２５】次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１２６】これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１２７】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１２８】相互認証が成功すれば、上位機器２０はサービスセンタ１０に対して機器認証開始を制御対象機器（下位機器）３０の代理として要求する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを上位機器２０に通知する。上位機器２０はサービスセンタ１０に制御対象機器（下位機器）３０の機器ＩＤを送信する。ここでサービスセンタ１０は下位機器の機器ＩＤの正当性を検証する。正当性の検証は、送付データ中に含まれる機器ＩＤがサービスセンタ１０の持つ機器情報データベース１０６に登録されているか否かをチェックする処理として実行される。機器Ｉ

Ｄの正当性検証が正常に終了すると、上位機器２０は制御対象機器（下位機器）３０にサービスセンタ１０との直接通信の許可を与える。これ以後、上位機器２０はサービスセンタ１０と制御対象機器（下位機器）３０との間の通信内容には関与しない。

【０１２９】サービスセンタ１０との直接通信許可を受けて、制御対象機器（下位機器）３０はセンタと直接通信して相互認証を行う。相互認証は、例えば前述の図２０、または図２２の例のいずれかを用いて実行される。相互認証が完了すると、以後の相互認証時に生成したセッション鍵（共通鍵）を用いてデータが暗号化されて送受信される。セッション鍵の生成はサービスセンタ１０、制御対象機器（下位機器）３０のどちらが行ってもよい。なお、ここではサービスセンタ１０と上位機器２０との間および上位機器２０と制御対象機器（下位機器）３０の間でそれぞれ相互認証が完了しているので、サービスセンタ１０と制御対象機器（下位機器）３０との直接の相互認証を省略することも可能である。相互認証やセッション鍵の交換が失敗した場合には、センタは下位機器にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は制御対象機器（下位機器）３０に処理完了を通知する。セッション鍵が制御対象機器（下位機器）３０とサービスセンタ１０の間で共有できれば、オンライン型下位機器は以降で説明する各手続きにおいて上位機器２０と同様に扱うことができる。

【０１３０】なお、暗号化機能を持たない制御対象機器（下位機器）３０の場合には、例えばワンタイムパスワードを用いた認証処理により制御対象機器（下位機器）３０の認証を実行する。この場合、サービスセンタ１０または、上位機器２０がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ１０と上位機器２０間のデータ通信をセッション鍵を用いたデータ通信とする。この場合のプロトコルを図２３に示す。

【０１３１】ｂ－２．オフライン型下位機器

次に、オフライン型下位機器の機器認証プロトコルについて説明する。この場合のプロトコルを図２４に示す。オフライン型の制御対象機器（下位機器）３０は、先に説明したようにメモリーカード等の情報記録媒体を介して制御情報を受け取る構成である。

【０１３２】オフライン型の制御対象機器（下位機器）３０は、最初に情報記録媒体が下位機器に装着されていなければ装着する。その場合には記録媒体の認証を行なう。この認証処理は、制御対象機器（下位機器）３０と情報記録媒体の構成（暗号処理機能、鍵格納構成）に応じて、前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。記録媒体認証が成功すると、制御対象機器（下位機器）３０は機器ＩＤなどの機器認証に必要なデータを情報記録媒体に転送する。転送が終了すると、情報記録媒体を上位機器２０に移動する。

【０１３３】上位機器２０は情報記録媒体がセットされると、情報記録媒体の認証を行った後、媒体から機器認証に必要なデータを転送する。情報記録媒体の認証処理は、制御対象機器（下位機器）３０と情報記録媒体との認証処理と同様前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。転送が終了すると上位機器２０と制御対象機器（下位機器）３０との相互認証が情報記録媒体の格納データに基づいて実行される。この間、情報記録媒体の上位機器２０と制御対象機器（下位機器）３０間での移動が必要であれば行う。相互認証が成功すれば、上位機器２０はサービスセンタ１０に機器認証開始を制御対象機器（下位機器）３０に代わって要求する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを上位機器２０に通知する。

【０１３４】次に、上位機器２０はサービスセンタ１０に制御対象機器（下位機器）３０の機器ＩＤを送信する。ここでサービスセンタ１０は制御対象機器（下位機器）３０の機器ＩＤの正当性を検証する。機器ＩＤの正当性検証が正常に終了すれば、制御対象機器（下位機器）３０はサービスセンタ２０と相互認証処理およびセッション鍵の交換を行う。しかし制御対象機器（下位機器）３０とサービスセンタ１０とは直接通信できないため、上位機器２０、および情報記録媒体が介在して行う。この間、必要に応じて情報記録媒体の上位機器２０と制御対象機器（下位機器）３０間での移動が行われる。相互認証が完了すると、以後のデータの暗号化に必要なセッション鍵（共通鍵）を生成する。セッション鍵の生成はサービスセンタ１０、制御対象機器（下位機器）３０のどちらが行ってもよい。なお、暗号化機能を持たない制御対象機器（下位機器）３０の場合には、例えばワンタイムパスワードを用いた認証処理により制御対象機器（下位機器）３０の認証を実行する。この場合、サービスセンタ１０または、上位機器２０がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ１０と上位機器２０間のデータ通信をセッション鍵を用いたデータ通信とする。相互認証やセッション鍵の交換が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は上位機器２０に処理完了を通知する。上位機器２０は情報記録媒体に処理完了通知もしくはエラー通知を転送する。情報記録媒体が制御対象機器（下位機器）３０に移動されると、制御対象機器（下位機器）３０は情報記録媒体を認証し、記録媒体から処理完了通知もしくはエラー通知を転送（読み出し処理）する。

【０１３５】［利用者登録、情報変更プロトコル］次に、利用者名や決済情報などの利用者情報をサービスセンタ１０の利用者情報データベース１０７（図５参照）に登録するための利用者登録、情報変更プロトコルについて説明する。

【０１３６】ａ．上位機器、オンライン型下位機器
まず上位機器２０およびオンライン型の制御対象機器（下位機器）３０の場合の処理について述べる。この場合のプロトコルを図２５に示す。上位機器２０およびオンライン型の制御対象機器（下位機器）３０は、「機器」と総称する。機器はサービスセンタ１０に対して利用者登録の開始要求を行う。サービスセンタ１０は利用者情報登録を行える状態であれば、機器に対して開始確認を通知する。機器は利用者が入力した利用者情報をセッション鍵で暗号化し、機器ＩＤとともに送信する。利用者情報は、氏名や住所、決済情報などである。決済情報は銀行口座、クレジットカード番号、プリペイドカード番号など、有償サービスの決済に必要な情報である。サービスセンタ１０は暗号化された利用者情報を、機器ＩＤに対応したセッション鍵で復号する。

【０１３７】続いてサービスセンタ１０は当該利用者に利用者ＩＤを発行し、その利用者ＩＤおよび利用者情報、機器ＩＤをサービスセンタ１０は内の利用者情報データベース１０７に登録する。データベースへの利用者情報の登録後、サービスセンタ１０は利用者ＩＤをセッション鍵で暗号化し、機器に送信する。機器はこれを受け取ると、暗号化された利用者ＩＤをセッション鍵で復号する。そして利用者ＩＤを利用者に通知する。通知は、制御対象機器（下位機器）３０の例えば表示部３０３（図３参照）において実行される。なお、上位機器において表示することも可能である。ここで利用者が機器を利用するたびに利用者ＩＤを入力する手間を省くために、利用者ＩＤを機器に保存しておき、利用者が自分のＩＤを選択するという方法をとってもよい。最後にサービスセンタ１０は機器に対して、処理完了通知もしくはエラー通知を行う。

【０１３８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず送受信し、上位機器２０がデータをセッション鍵で暗号化した後、サービスセンタ１０に送信する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、下位機器に送信する。この場合のプロトコルを図２６に示す。

【０１３９】なお、すでにサービスセンタ１０内の利用者情報データベース１０７に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者ＩＤを発行すること、および利用者ＩＤを上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者ＩＤを入力してもよい。この時、サービスセンタ１０は、利用者が利用している機器の機器ＩＤが当該の利用者ＩＤと関連づけられていなければ、利用者情報データベース１０７に機器ＩＤを追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図２７に示す。

【０１４０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図２８に示す。

【０１４１】ｂ．オフライン型下位機器
続いてオフライン型下位機器の場合について述べる。この場合のプロトコルを図２９に示す。記録媒体がオフライン型の制御対象機器（下位機器）３０に装着されていなければ装着する。その場合には記録媒体の認証が必要となる。制御対象機器（下位機器）３０は利用者が入力した利用者情報をセッション鍵で暗号化した後、機器ＩＤとともに情報記録媒体に転送する。転送が完了した後、情報記録媒体を制御対象機器（下位機器）３０から取り外し、上位機器２０に装着する。

【０１４２】上位機器２０は情報記録媒体が装着されると、情報記録媒体の認証を開始する。情報記録媒体の認証が終了した後、上位機器２０は情報記録媒体からデータを転送（読み取り）する。転送終了後、上位機器２０はサービスセンタ１０に利用者登録開始要求を下位機器の代理として行う。サービスセンタ１０は利用者情報登録を行える状態であれば、上位機器２０に対して開始確認を通知する。

【０１４３】上位機器２０は制御対象機器（下位機器）３０からのデータをそのままサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者情報を機器ＩＤに対応したセッション鍵で復号する。続いて当該利用者に利用者ＩＤを発行し、その利用者ＩＤおよび利用者情報、機器ＩＤを利用者情報データベース１０７に登録する。

【０１４４】サービスセンタ１０はデータベースへの利用者情報の登録後、利用者ＩＤを制御対象機器（下位機器）３０とのセッション鍵で暗号化し、上位機器２０に送信する。そしてサービスセンタ１０は上位機器２０に対して、処理完了通知もしくはエラー通知を行う。上位機器２０は、サービスセンタ１０から処理完了通知を受け取ると暗号化された利用者ＩＤを情報記録媒体に転送する。その後、情報記録媒体を上位機器２０から制御対象機器（下位機器）３０に移動する。情報記録媒体が制御対象機器（下位機器）３０に装着されると、制御対象機器（下位機器）３０は情報記録媒体の認証を行う。認証が成功すれば、制御対象機器（下位機器）３０は情報記録媒体内のデータを転送（データ読み取り）する。

【０１４５】次に、制御対象機器（下位機器）３０は情報記録媒体から読み取った暗号化された利用者ＩＤをセッション鍵で復号する。そして利用者ＩＤを利用者に通知する。通知は、制御対象機器（下位機器）３０の例え

ば表示部３０３（図４参照）において実行される。ここで利用者が機器を利用するたびに利用者ＩＤを入力する手間を省くために、利用者ＩＤを機器に保存しておき、それを利用者が自分のＩＤを選択するという方法をとってもよい。

【０１４６】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３０に示す。

【０１４７】なお、すでにサービスセンタ１０内の利用者情報データベース１０７に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者ＩＤを発行すること、および利用者ＩＤを上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者ＩＤを入力してもよい。この時、サービスセンタ１０は、利用者が利用している機器の機器ＩＤが当該の利用者ＩＤと関連づけられていなければ、利用者情報データベース１０７に機器ＩＤを追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図３１に示す。

【０１４８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３２に示す。

【０１４９】［利用者認証情報登録プロトコル］利用者を識別するためにはいくつかの方法が考えられるが、ここではパスワードを用いた方法とＩＤカードを用いた場合について説明する。ＩＤカードを用いる場合には、個人別のＩＤを埋め込んだカード、指紋などの生体情報を認識できる機構を備えたカード、あるいは利用者個人の公開鍵・秘密鍵の組を保存しているカードなどを用いることが可能である。ＩＤカードとしては磁気テープを有する接触型カードや、無線通信を行う非接触型カードのどちらを用いてもよい。また、利用者を識別するための利用者認証情報を保存し照合を行う場所としては、機器（上位機器・制御対象機器（下位機器））あるいはサービスセンタが考えられる。機器に保存する場合は機器における利用者の制限などの管理を個別に行うことが容易である。サービスセンタに登録する場合には複数の機器を利用する場合においても、機器ごとに登録作業を行う必要がない。まずパスワード等、認証のための情報を機器もしくはセンタに登録する手続きについて述べる。

【０１５０】ａ．機器に保存

利用者のパスワード等の利用者認証情報を機器内部に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３３に示す。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。

【０１５１】利用者がパスワードを操作部（上位機器の場合、操作部２０９、下位機器の場合操作部３０８）から入力すると、機器は利用者ＩＤと対応するパスワードの組を機器内部のメモリに保存する。この時、パスワードを平文のまま保存するのではなく暗号化を施してもよい。次に、サービスセンタ１０は機器に対して、処理完了もしくはエラーを通知する。

【０１５２】次にＩＤカードを用いる利用者認証情報登録処理について説明する。この場合のプロトコルを図３４に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器は利用者ＩＤと対応する利用者認証情報を機器内部のメモリに保存する。次にサービスセンタ１０は機器に対して、処理完了もしくはエラーを通知する。

【０１５３】ｂ．センタに保存（上位機器・オンライン型下位機器）

利用者認証情報をサービスセンタ１０に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３５に示す。

【０１５４】まず上位機器およびオンライン型の制御対象機器（下位機器）を利用する場合は以下の通りである。機器はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者ＩＤと対応するパスワードの組をセッション鍵で暗号化し、機器ＩＤとともにサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。続いて、パスワードを利用者情報データベース１０７に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ１０は機器にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は機器に処理完了を通知する。

【０１５５】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗

号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３６に示す。

【０１５６】次に、ＩＤカードを用いる方法について説明する。この場合のプロトコルを図３７に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。その後、機器は利用者ＩＤと対応する利用者認証情報の組をセッション鍵で暗号化し、機器ＩＤとともにサービスセンタ１０に送信する。以下の処理はパスワードを用いる場合と同様である。

【０１５７】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３８に示す。

【０１５８】ｃ．オフライン型下位機器

次にオフライン型の制御対象機器（下位機器）の場合の利用者認証情報登録プロトコルについて述べる。まず、この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３９に示す。

【０１５９】オフライン型の制御対象機器（下位機器）３０は利用者に利用者ＩＤおよびパスワードの入力を促す。利用者ＩＤおよびパスワードが入力されると、制御対象機器（下位機器）３０はこれをセッション鍵で暗号化して機器ＩＤとともに情報記録媒体に転送する。情報記録媒体が下位機器から上位機器に移されると、上位機器２０は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器２０は情報記録媒体からデータを転送する。その後、上位機器２０はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを上位機器２０に通知する。上位機器２０は情報記録媒体から転送（読み出し）したデータをそのままセンタに送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。続いて、パスワードを利用者情報データベース１０７に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は上位機器２０に処理完了を通知する。サービスセンタ１０から上位機器２０に対するエラー通知、処理完了通知は情報記録媒体を介してオフライン型の制御対象機器（下位機器）３０に転送される。

【０１６０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４０に示す。

【０１６１】次に、ＩＤカードを用いる利用者認証情報登録プロトコルについて説明する。この場合のプロトコルを図４１に示す。制御対象機器（下位機器）３０は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。

【０１６２】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４２に示す。

【０１６３】［利用者認証プロトコル］次に、利用者認証情報登録プロトコルで登録した利用者認証情報を用いて、利用者を認証する手続きについて述べる。

【０１６４】ａ．機器に利用者認証情報を保存

利用者の利用者認証情報を機器に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する場合の利用者認証の方法について説明する。

【０１６５】利用者認証情報としてパスワードを利用する場合のプロトコルを図４３に示す。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器はメモリに保存されている利用者ＩＤとパスワードの組の中から、利用者ＩＤに対応したパスワードを選び出し、これと入力されたパスワードとを照合する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【０１６６】次にＩＤカードを用いる方法について説明する。この場合のプロトコルを図４４に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。この後、機器は内部のメモリに保存されている利用者ＩＤと利用者認証情報の組の中から、利用者ＩＤに対応した利用者認証情報を選び出し、ＩＤカードから転送した利用者認証情報を照合する。照合に成功すれば利用者は正当な権限を

有すると言え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【０１６７】ｂ．センタに利用者認証情報を保存

利用者のパスワードをサービスセンタ１０に保存して、サービスの提供等の際に利用者の入力したパスワードと照合する場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図４５に示す。機器はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者ＩＤと対応するパスワードの組をセッション鍵で暗号化した上で機器ＩＤと共にセンタに送信する。センタは暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は機器・利用者情報データベース１０７に登録されたパスワードと、機器から送信されたパスワードとを照合する。サービスセンタ１０は照合結果を機器に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース１０７の当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。このことにより利用者が複数の機器を利用する場合にも、利用者ＩＤと機器ＩＤとを関連づけることが可能である。照合に失敗した場合はエラー処理を行う。

【０１６８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４６に示す。

【０１６９】次に、ＩＤカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図４７に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者ＩＤと対応する利用者認証情報の組をセッション鍵で暗号化した上で機器ＩＤと共にサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤと利用者認証情報を機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は利用者情報データベース１０７に登録された利用者認証情報と、機器から送信された利用者認証情報とを照合する。さらに、サービスセンタ１０は照合結果を機器に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース１０７の当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。

【０１７０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４８に示す。

【０１７１】ｃ．オフライン型の下位機器の場合

次にオフライン型の制御対象機器（下位機器）３０の場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図４９に示す。オフライン型の制御対象機器（下位機器）３０は利用者に利用者ＩＤおよびパスワードの入力を促す。利用者ＩＤおよびパスワードが入力されれば、制御対象機器（下位機器）３０はこれをセッション鍵で暗号化して機器ＩＤとともに情報記録媒体に転送する。

【０１７２】情報記録媒体が制御対象機器（下位機器）３０から上位機器２０に移されると、上位機器２０は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器２０は情報記録媒体からデータを転送（読み取り）する。そして、上位機器２０はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、認証開始可能であることを上位機器２０に通知する。通知を受領すると上位機器２０は情報記録媒体から転送したデータをそのままサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は利用者情報データベース１０７に登録された利用者認証情報と、機器から送信された利用者認証情報とを照合する。サービスセンタ１０は照合結果を上位機器２０に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベースの当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。認証結果を受け取った上位機器２０は、情報記録媒体にその結果を転送する。情報記録媒体が上位機器２０から制御対象機器（下位機器）３０に移されると、制御対象機器（下位機器）３０は情報記録媒体の認証を行う。記録媒体認証が成功すれば、下位機器は情報記録媒体からデータを転送（読み取り）する。制御対象機器（下位機器）３０は認証結果を利用者に、例えば表示部３０３を介して通知する。

【０１７３】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５０に示す。

【０１７４】次にオフライン型の制御対象機器（下位機器）３０の場合におけるＩＤカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図５１に示す。オフライン型の制御対象機器（下位機器）３０は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。

【０１７５】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５２に示す。

【０１７６】［サービスプロトコル］次に、サービスセンタ１０から上位機器２０を利用した遠隔サービスの提供処理について説明する。

【０１７７】ａ．センター上位機器、センター上位機器－下位機器（オンライン）

まず、サービスセンタ１０と上位機器２０、オンライン型の制御対象機器（下位機器）３０を利用する場合のプロトコルを図５３に示す。ここでは、機器といった場合、上位機器２０と、オンライン型の制御対象機器（下位機器）３０とを含む総称である。

【０１７８】最初に機器はサービスセンタ１０にサービス開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、サービス開始可能であることを機器に通知する。サービスはサービスセンタ１０と機器との間でデータを通信することにより実施される。サービスセンタ１０からサービス提供のためのデータが送信される場合について述べる。

【０１７９】まずサービスセンタのＣＰＵ１０１の制御によりサービス提供用データベース１０３から、例えばメンテナンス情報のようなサービス用データが暗号化通信ＩＣ１０４に送られる。暗号化通信ＩＣ１０４は、そのデータを機器認証の際にサービスセンタと機器との間で交換したセッション鍵により暗号化を施した後、外部ネットワークインタフェース１０５を経由して外部ネットワークに送信する。

【０１８０】上位機器２０側では、暗号化通信ＩＣ２０５が外部ネットワークインタフェース２０８経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じてメモリ２０２やディスク等の記録装置２１０に転送される。ＣＰＵ２０１はメモリ２０２やディスク等の記録装置２１０からデータを読み出して、機器固有部２０４の制御を行う。なお、オンライン型の制御対象機器（下位機器）３０の制御を行なう場合は、上位機器２０と制御対象機器（下位機器）３０間でデータが転送される。

【０１８１】続いてオンライン型の制御対象機器（下位機器）３０からサービスセンタ１０にデータを送信する場合について述べる。まず、オンライン型の制御対象機器（下位機器）３０のＣＰＵ３０１の制御によりデータが暗号化通信ＩＣ３０５に送られる。暗号化通信ＩＣ３０５は、データのセッション鍵による暗号化を施した後、ローカルインタフェース３０７を介して上位機器２０に送信する。上位機器２０は制御対象機器（下位機器）３０からローカルインタフェース２０８を介して受信したデータを外部ネットワークインタフェース２０８を経由して外部ネットワークに送信する。

【０１８２】サービスセンタ１０側では、暗号化通信ＩＣ１０４が外部ネットワークインタフェース１０５経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ１０２やサービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７に転送される。サービスを提供している間、必要であればサービスセンタ１０のＣＰＵ１０１は課金情報をメモリ１０２もしくは利用者情報データベース１０７に記録する。課金情報とは有償サービスの利用回数や時間、送受信データ量などである。

【０１８３】以上、説明したように、サービスの提供中にサービスセンタ１０と機器との間で行われるデータの通信は、セッション鍵を用いて暗号化されているので通信内容の保護が可能となる。サービスの提供が終了すれば、サービスセンタ１０のＣＰＵ１０１は利用者ＩＤを検索キーとして利用者データベースから利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。

【０１８４】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図５４に示す。

【０１８５】２．センター上位機器－下位機器（オフライン）

次に、オフライン型下位機器に対する遠隔サービスの提供処理について説明する。この場合、サービスはサービ

スセンタ１０と上位機器２０との間で通信を行い、上位機器２０がオフライン型の制御対象機器（下位機器）３０の代わりにデータを受信して一度保存し、そのデータを情報記録媒体を用いてまとめて下位機器に転送することにより実施される。この場合のプロトコルを図５５に示す。

【０１８６】最初に情報記録媒体が制御対象機器（下位機器）３０に装着されていなければ装着する。その場合には情報記録媒体の認証が必要となる。情報記録媒体の認証が成功すると、制御対象機器（下位機器）３０はサービス名やパラメータなど、サービス開始に必要なデータを媒体に転送する。転送が終了してから、情報記録媒体を上位機器２０に移動する。

【０１８７】上位機器２０は情報記録媒体がセットされると、情報記録媒体認証を行った後、情報記録媒体からサービス開始に必要なデータを転送する。転送が終了すると上位機器２０はサービスセンタ１０にサービス開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、サービス開始可能であることを上位機器２０に通知する。

【０１８８】サービス提供中にデータを上位機器２０と制御対象機器（下位機器）３０との間でやりとりする場合について述べる。上位機器２０が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、上位機器２０の暗号化通信ＩＣ２０５は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、上位機器２０のＣＰＵ２０１はサービスセンタ１０から制御対象機器（下位機器）３０のために受信したデータを上位機器２０内部の記録装置２１０から読み出し、暗号化通信ＩＣ２０５に転送する。暗号化通信ＩＣ２０５に転送されたデータはそのまま記録媒体インタフェース２０７を経由して情報記録媒体２１１に転送（書き込み）される。

【０１８９】制御対象機器（下位機器）３０が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、制御対象機器（下位機器）３０のＣＰＵ３０１はメモリ３０２もしくは記録装置３０９からデータを読み出し、暗号化通信ＩＣ３０５に転送する。暗号化通信ＩＣ３０５は転送されたデータをセッション鍵で暗号化し、記録媒体インターフェース３０６経由で情報記録媒体３１０に転送する。

【０１９０】またサービス提供中にデータをサービスセンタ１０と上位機器２０の間でやりとりする場合について述べる。サービスセンタ１０からサービス提供のためのデータが送信される場合について述べる。最初にサービスセンタ１０のＣＰＵ１０１の制御によりサービス提供用データベース１０３からデータが暗号化通信ＩＣ１０４に送られる。暗号化通信ＩＣ１０４は、そのデータを機器認証の際にサービスセンタ１０と制御対象機器（下位機器）３０との間で交換したセッション鍵により暗号化を施した後、外部ネットワークインタフェース１０５を経由して外部ネットワークに送信する。

【０１９１】上位機器２０側では、暗号化通信ＩＣ２０５が外部ネットワークインタフェース２０８経由でデータを受信し、データバスを通じてメモリ２０２やディスク等の記録装置２１０に転送する。

【０１９２】続いて上位機器２０からサービスセンタ１０にデータを送信する場合について述べる。まず、上位機器２０のＣＰＵ２０１の制御により制御対象機器（下位機器）３０とサービスセンタ１０との間で交換されたセッション鍵で暗号化されたデータは、メモリ２０２もしくは記録装置２１０から読み出されて暗号化通信ＩＣ２０５に送られる。暗号化通信ＩＣ２０５はそのデータを外部ネットワークインタフェース２０６を経由して外部ネットワークに送信する。サービスセンタ１０側では、暗号化通信ＩＣ１０４が外部ネットワークインタフェース１０５経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ１０２やサービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７に転送される。サービスを提供している間、必要であればサービスセンタ１０のＣＰＵ１０１は課金情報をメモリ１０２もしくは利用者情報データベース１０７に記録する。課金情報とは有償サービスの利用回数や時間、送受信データ量などである。

【０１９３】以上のように、サービスの提供中にサービスセンタと機器との間で行われるデータの通信は、セッション鍵を用いて暗号化され通信内容を保護することができる。サービスの提供が終了すれば、サービスセンタ１０のＣＰＵ１０１は利用者ＩＤを検索キーとして利用者データベース１０７から利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。

【０１９４】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５６に示す。

【０１９５】［具体的処理例］以下、本発明の通信手段を介したサービス提供システムおよびサービス提供方法の具体的なサービス提供例について説明する。

【０１９６】＜リモートメンテナンス＞まず、具体的なサービス提供例として、遠隔診断・修復システムについて述べる。この場合のプロトコルを図５７に示す。このシステムは、機器に障害が発生した場合に、障害個所の

診断及び修復をサービスセンタ１０からの操作により行う例である。

【０１９７】まず機器の状態を調べるために診断を行う。この診断は、機器のＣＰＵ（上位機器の場合はＣＰＵ２０１、下位機器の場合はＣＰＵ３０１）が機器内部の様々な部分に対して命令を発行してその応答を分析することによっておこなう。診断のためのプログラムは機器内部のメモリやディスク等に予め記録しておく。診断が終了すれば、その結果をサービスセンタ１０に送信する。あるいはセンタの助けを借りて診断を行う構成としてもよい。この場合、機器はサービスセンタ１０に対して診断依頼のメッセージを送信する。診断依頼のメッセージを受け取ったサービスセンタ１０は、該当機器の診断が可能であれば診断命令を発行し、機器に対して送信する。機器はサービスセンタ１０から診断命令を受け取るとその命令を実行し、結果をサービスセンタ１０に送信する。

【０１９８】サービスセンタ１０は機器から送信された結果を分析し、それによって必要ならば再度診断命令を発行し、機器に送信する。サービスセンタ１０が診断が終了したと判断できるまで、上記診断命令の発行から分析の手順を繰り返す。以上のように遠隔診断を行って障害箇所および状態を特定でき、かつ遠隔修復が可能であれば修復の手続きに入る。遠隔修復は診断結果に基づき、サービスセンタ１０が機器の障害を復旧するために必要な修復命令を機器に送信することにより行われる。

【０１９９】サービスセンタ１０のＣＰＵ１０１は診断結果を分析して、修復命令を発行する。この際サービス提供用データベース１０３に蓄積された該当機器あるいは同機種の過去の障害履歴を参照して、最適な命令を選択する。サービスセンタ１０はこの修復命令を機器に送信する。機器は受信した修復命令を機器内のＣＰＵの制御により実行してその結果をセンタに送信する。結果を受信したサービスセンタは、その結果や過去の履歴に基づいて分析を行い、必要ならば再度修復命令を発行し、機器に送信する。必要に応じて利用者へのメッセージを機器の表示部に表示する。そして修復の実行を続けるなどの入力を求める。センタが修復が完了したと判断する、あるいは利用者が修復を終了するまで、上記修復命令の発行から分析の手順を繰り返す。修復を終了する際には、それまでの診断結果および修復内容を機器情報データベース１０６に登録する。データベースに登録された診断結果および修復内容は課金に利用したり、複数の機器のデータをまとめて機器メーカーへフィードバックして機器の改善に役立てたりすることが可能である。そしてセンタは機器に対して遠隔修復の終了を通知する。

【０２００】＜バックアップ・リストア＞本発明の別のサービス提供例として、機器に保存されているデータのバックアップおよびリストア処理をサービスセンタ１０が実行する処理構成について説明する。

【０２０１】これは、機器に保存されている設定情報等のデータをあらかじめサービスセンタ１０の記憶手段にバックアップしておき、データが万一消失してもリストアすることで、その機器を以前の状態のまま利用できるようにするためのものである。最初にバックアップについて説明する。この場合のプロトコルを図５８に示す。

【０２０２】機器はサービスセンタ１０に対してバックアップ開始要求を行う。この要求を受信したサービスセンタ１０は、サービス提供用データベース１０３上にバックアップのための領域の確保を行う。領域確保が成功し、かつバックアップを行える状態にあれば、サービスセンタ１０は機器に対してバックアップ開始確認通知を送信する。開始確認通知を受信した機器は、バックアップ対象のデータをサービスセンタ１０に送信する。サービスセンタ１０は受信したバックアップデータを確保した領域に保存する。保存が終了すると、機器情報データベース１０６にバックアップ日時や保存領域などのバックアップ情報を登録する。そしてサービスセンタ１０は機器に対してバックアップの終了を通知する。

【０２０３】続いてリストアの手順について説明する。この場合のプロトコルを図５９に示す。機器はサービスセンタ１０に対してリストア開始要求を行う。この要求を受信したサービスセンタ１０は、機器ＩＤを検索キーとして機器情報データベース１０６からバックアップ情報を取得する。バックアップ情報の取得に成功し、かつリストアを行える状態にあれば、サービスセンタ１０は機器に対してリストア開始確認通知を送信する。そしてサービスセンタ１０は、バックアップ情報からバックアップデータが保存されているサービス提供用データベース１０３上の領域情報を取り出す。この情報に基づきサービス提供用データベース１０３上の領域からバックアップデータを読み出し、機器に送信する。

【０２０４】機器は受信したバックアップデータをチェックした後、リストアを実行する。リストアが終了すると、機器はサービスセンタ１０に対してリストアの終了を通知する。リストア終了通知を受信したサービスセンタ１０は、機器情報データベース１０６にリストア履歴を登録する。そしてサービスセンタ１０は機器に対してリストアに関する処理の終了を通知する。

【０２０５】＜データ配信（音楽、映像、文字情報など）＞本発明のさらに別のサービス提供例として、データ配信について述べる。

【０２０６】これは、音楽や映像、文字情報などのデータをサービスセンタ１０に蓄積し、利用者の要求に応じてサービスセンタ１０から機器に取り込んで利用できるものである。この場合のプロトコルを図６０に示す。データ配信機能を利用する場合には、まず利用者は機器に設けられた操作部（上位機器の場合は操作部２０９、下位機器の場合は操作部３０８）でデータ配信を開始する操作を行う。利用者からの入力を受け付けた機器はサー

ビスセンタ１０に対してデータ配信開始要求を行う。サービスセンタ１０は、データ配信を行える状態にあれば、機器に対してデータ配信開始確認通知を送信する。開始確認通知を受信した機器は、表示部（上位機器の場合は表示部２０３、下位機器の場合は表示部３０３）にデータ配信開始のメッセージを表示する。さらにサービスセンタ１０は利用可能なデータに関する選択肢を含んだメニューを機器に送信する。機器はこのメニューを受信すると、表示部に出力する。

【０２０７】利用者がメニューの中から必要なデータを選択して操作部に入力すると、機器は選択されたデータが何であるかという情報、たとえばデータ番号をサービスセンタ１０に送信する。サービスセンタ１０は、サービス提供用データベースから必要なデータを取得し、機器に送信する。機器はデータを受信したことを表示部に出力する。そして利用者はデータを再生するなどの操作を行う。利用者が引き続きデータ配信機能を利用する場合には、操作部から必要な入力を行えばよい。データ配信が終了すると、サービスセンタ１０は、必要であれば機器情報データベース１０６にデータ配信履歴を登録する。データベースに登録されたデータ配信履歴は課金に利用したり、複数の機器のデータをまとめて以後提供するデータの検討などのマーケティングに役立てたりすることが可能である。そしてサービスセンタ１０は機器に対してデータ配信の終了を通知する。

【０２０８】＜ヘルプ・チュートリアル＞さらに、本発明の別のサービス提供例として、機器の操作方法を解説するヘルプ機能を提供する例について述べる。これは、機器の操作方法を解説するヘルプデータをサービスセンタ１０に蓄積し、利用者の要求に応じて必要な部分を機器に取り込んで、利用者に提示するものである。この場合のプロトコルを図６１に示す。

【０２０９】このヘルプ機能に関しては、機器にすべてのヘルプデータを保存しておくことも可能であるが、機器には保存のための領域が少ない場合があることや、常に新しいヘルプデータを保持することが困難なことから、全部あるいは一部のヘルプデータをサービスセンタ１０に置く形態とする例である。ヘルプ機能を利用する場合には、まず利用者は操作部（上位機器の場合は操作部２０９、下位機器の場合は操作部３０８）でヘルプを開始する操作を行う。利用者からの入力を受け付けた機器はサービスセンタ１０に対してヘルプ開始要求を行う。ヘルプデータの提供を行える状態にあれば、サービスセンタ１０は機器に対してヘルプ開始確認通知を送信する。

【０２１０】開始確認通知を受信した機器は、ヘルプの必要な部分を指定するデータをサービスセンタ１０に送信する。これを受信したサービスセンタ１０は、サービス提供用データベース１０３から必要なヘルプデータを取得し、機器に送信する。機器は受信したヘルプデータを表示部（上位機器の場合は表示部２０３、下位機器の場合は表示部３０３）に表示する。利用者が引き続きヘルプ機能を利用する場合には、操作部から必要な入力を行えばよい。ヘルプデータの提供が終了すると、機器情報データベースにヘルプ提供履歴を登録する。そしてセンタは機器に対してヘルプの終了を通知する。

【０２１１】また単純なヘルプだけではなく、チュートリアルを提供する、すなわち操作情報を提供する構成とすることも可能である。これは利用者が機器の利用方法を習得するための機能であり、機器の各部分を操作するとその状況に応じて、表示や操作形態が変化する。この場合のプロトコルを図６２に示す。チュートリアル機能を利用する場合には、まず利用者は操作部でチュートリアルを開始する操作を行う。利用者からの入力を受け付けた機器はセンタに対してチュートリアル開始要求を行う。チュートリアルを行える状態にあれば、センタは機器に対してチュートリアル開始確認通知を送信する。開始確認通知を受信した機器は、表示部にチュートリアル開始のメッセージを表示する。利用者が機器の操作を行うと、機器は操作内容と機器の内部状態をサービスセンタ１０に送信する。サービスセンタ１０はこれらの情報に基づいて、次に提供すべきデータを決定する。そして、サービス提供用データベースから必要なチュートリアルデータを取得し、機器に送信する。

【０２１２】機器は受信したチュートリアルデータを表示部に表示する。利用者が引き続きチュートリアル機能を利用する場合には、操作部から必要な入力を行えばよい。チュートリアルデータの提供が終了すると、機器情報データベースにチュートリアル提供履歴を登録する。そしてセンタは機器に対してチュートリアルの終了を通知する。

【０２１３】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２１４】

【発明の効果】以上説明してきたように、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、機器がサービスセンタと直接接続できない構成であった場合でも、通信手段を有する上位機器からローカルネットワークまたは情報記録媒体を介してサービスセンタからの情報を受け取ることが可能となり、制御、メンテナンス等の必要な制御対象機器（下位機器）のすべてに外部ネットワークに接続するための通信インタフェース等の通信手段を構成することが必要とならない。

【０２１５】さらに、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、制御、メンテナンス等の必要な制御対象機器（下位機器）が暗号化機能を備えない構成であっても、制御対象機器（下位機器）とローカルネットワークまたは情報記録媒体を介して通信可能な上位機器がデータを暗号化した上でサービスセンタとの通信処理を実行するため、通信データの安全性が保証されていない公衆ネットワークを経由しても、制御情報、あるいは制御情報を提供するために必要となる個人情報などの重要な情報の漏洩が防止可能となる。

【図面の簡単な説明】

【図１】本発明の通信手段を介したサービス提供システムのシステム概要を示す図である。

【図２】本発明の通信手段を介したサービス提供システムを構成する上位機器の構成を示す図である。

【図３】本発明の通信手段を介したサービス提供システムを構成する下位機器（オンライン型）の構成を示す図である。

【図４】本発明の通信手段を介したサービス提供システムを構成する下位機器（オフライン型）の構成を示す図である。

【図５】本発明の通信手段を介したサービス提供システムを構成するサービスセンタの構成を示す図である。

【図６】本発明の通信手段を介したサービス提供システムにおけるデータ通信の暗号化・認証レベルを示す図である。

【図７】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その１）である。

【図８】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その２）である。

【図９】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その３）である。

【図１０】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その４）である。

【図１１】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その１）である。

【図１２】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その２）である。

【図１３】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その３）である。

【図１４】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その４）である。

【図１５】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その５）である。

【図１６】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その６）である。

【図１７】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その７）である。

【図１８】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その８）である。

【図１９】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その１）である。

【図２０】本発明の通信手段を介したサービス提供システムにおいて適用可能な相互認証処理を説明する図である。

【図２１】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その２）である。

【図２２】本発明の通信手段を介したサービス提供システムにおいて適用可能な相互認証処理を説明する図である。

【図２３】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その３）である。

【図２４】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その４）である。

【図２５】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その１）である。

【図２６】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その２）である。

【図２７】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その１）である。

【図２８】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その２）である。

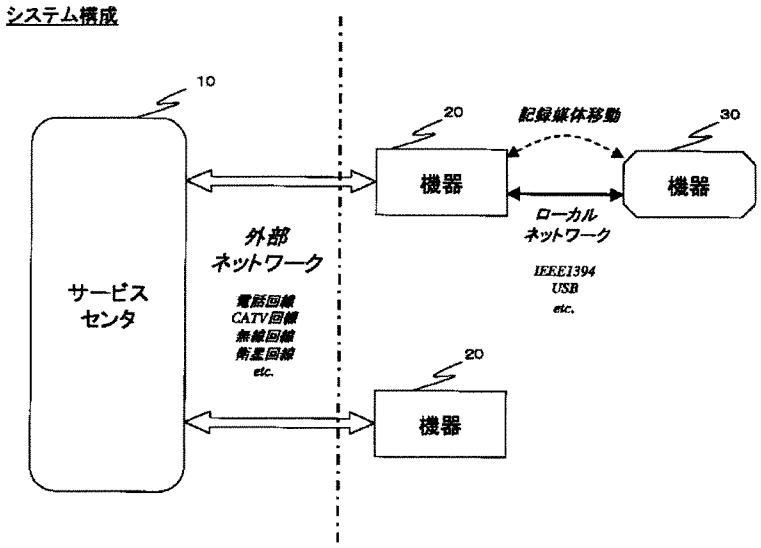
【図２９】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その３）である。

【図３０】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その４）である。

【図３１】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その３）である。
【図３２】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その４）である。
【図３３】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その１）である。
【図３４】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その２）である。
【図３５】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その３）である。
【図３６】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その４）である。
【図３７】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その５）である。
【図３８】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その６）である。
【図３９】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その７）である。
【図４０】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その８）である。
【図４１】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その９）である。
【図４２】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その１０）である。
【図４３】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その１）である。
【図４４】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その２）である。
【図４５】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その３）である。
【図４６】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その４）である。
【図４７】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その５）である。
【図４８】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その６）である。
【図４９】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その７）である。
【図５０】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その８）である。
【図５１】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その９）である。
【図５２】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その１０）である。
【図５３】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その１）である。
【図５４】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その２）である。
【図５５】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その３）である。
【図５６】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その４）である。
【図５７】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としての遠隔診断、修復処理を説明する図である。
【図５８】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのバックアップ処理を説明する図である。
【図５９】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのリストア処理を説明する図である。
【図６０】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのデータ配信処理を説明する図である。
【図６１】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのヘルプデータ提供処理を説明する図である。
【図６２】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのチュートリアル処理を説明する図である。
【符号の説明】
１０　サービスセンタ
２０　上位機器
３０　制御対象機器(下位機器)

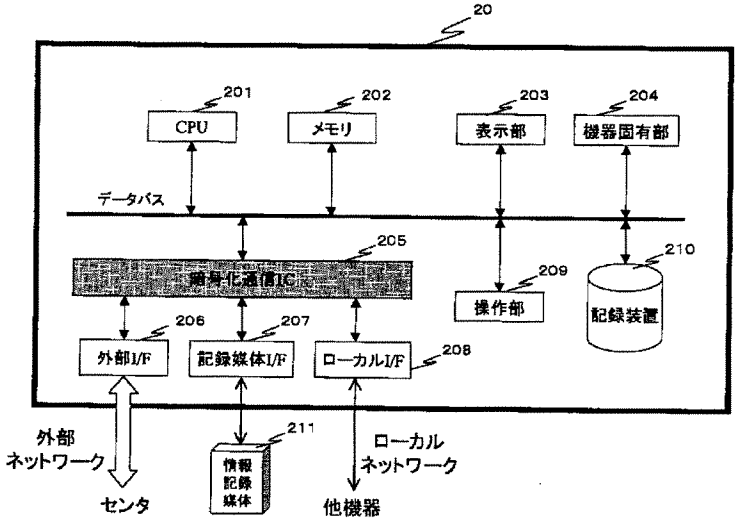
１０１　ＣＰＵ
１０２　メモリ
１０３　サービス提供用データベース
１０４　暗号化通信ＩＣ
１０５　外部インタフェース
１０６　機器情報データベース
１０７　利用者情報データベース
２０１　ＣＰＵ
２０２　メモリ
２０３　表示部
２０４　機器固有部
２０５　暗号化通信ＩＣ
２０６　外部インタフェース
２０７　記録媒体インタフェース
２０８　ローカルインタフェース
２０９　操作部
２１０　記録装置
２１１　情報記録媒体
３０１　ＣＰＵ
３０２　メモリ
３０３　表示部
３０４　機器固有部
３０５　暗号化通信ＩＣ
３０６　記録媒体インタフェース
３０７　ローカルインタフェース
３０８　操作部
３０９　記録装置
３１０　情報記録媒体

【図１】



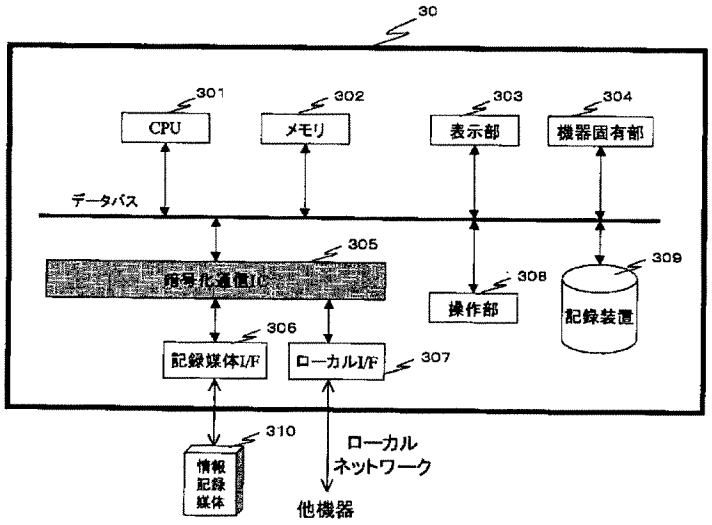
【図２】

上位機器

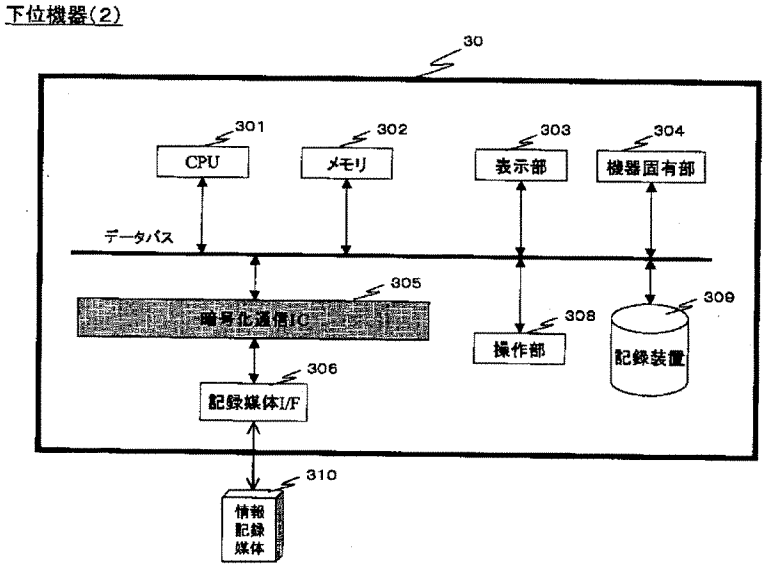


【図３】

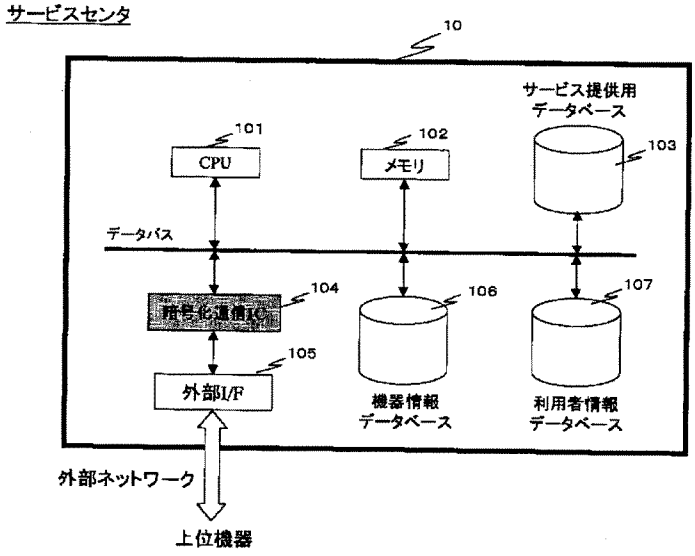
下位機器(1)



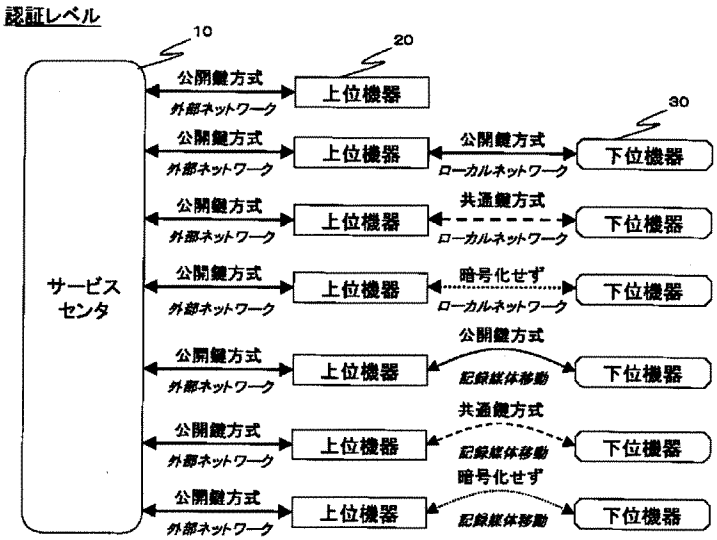
【図４】


下位機器(2)
30
301
CPU
302
メモリ
303
表示部
304
機器固有部
データバス
305
暗号化通信IC
306
記録媒体I/F
308
操作部
309
記録装置
310
情報記録媒体

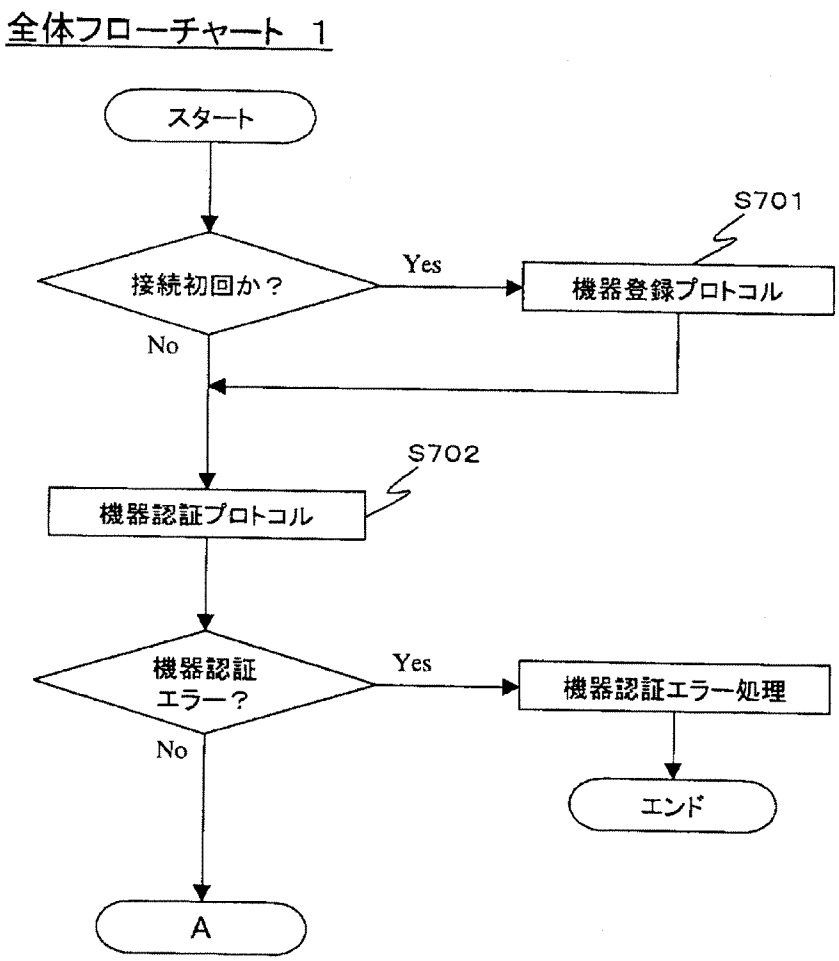
【図５】


サービスセンタ
10
サービス提供用データベース
101
CPU
102
メモリ
103
データバス
104
暗号化通信IC
105
外部I/F
106
機器情報データベース
107
利用者情報データベース
外部ネットワーク
上位機器

【図６】

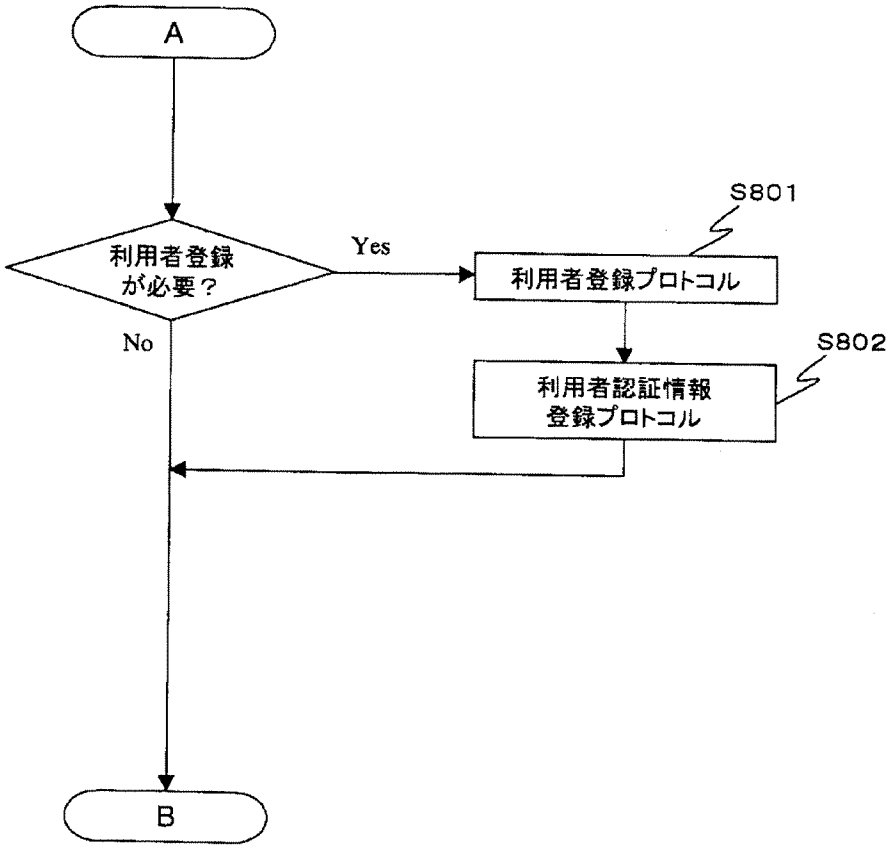

認証レベル
10
20
30
サービス
センタ
公開鍵方式
外部ネットワーク
上位機器
公開鍵方式
ローカルネットワーク
下位機器
共通鍵方式
暗号化せず
記録媒体移動

【図７】

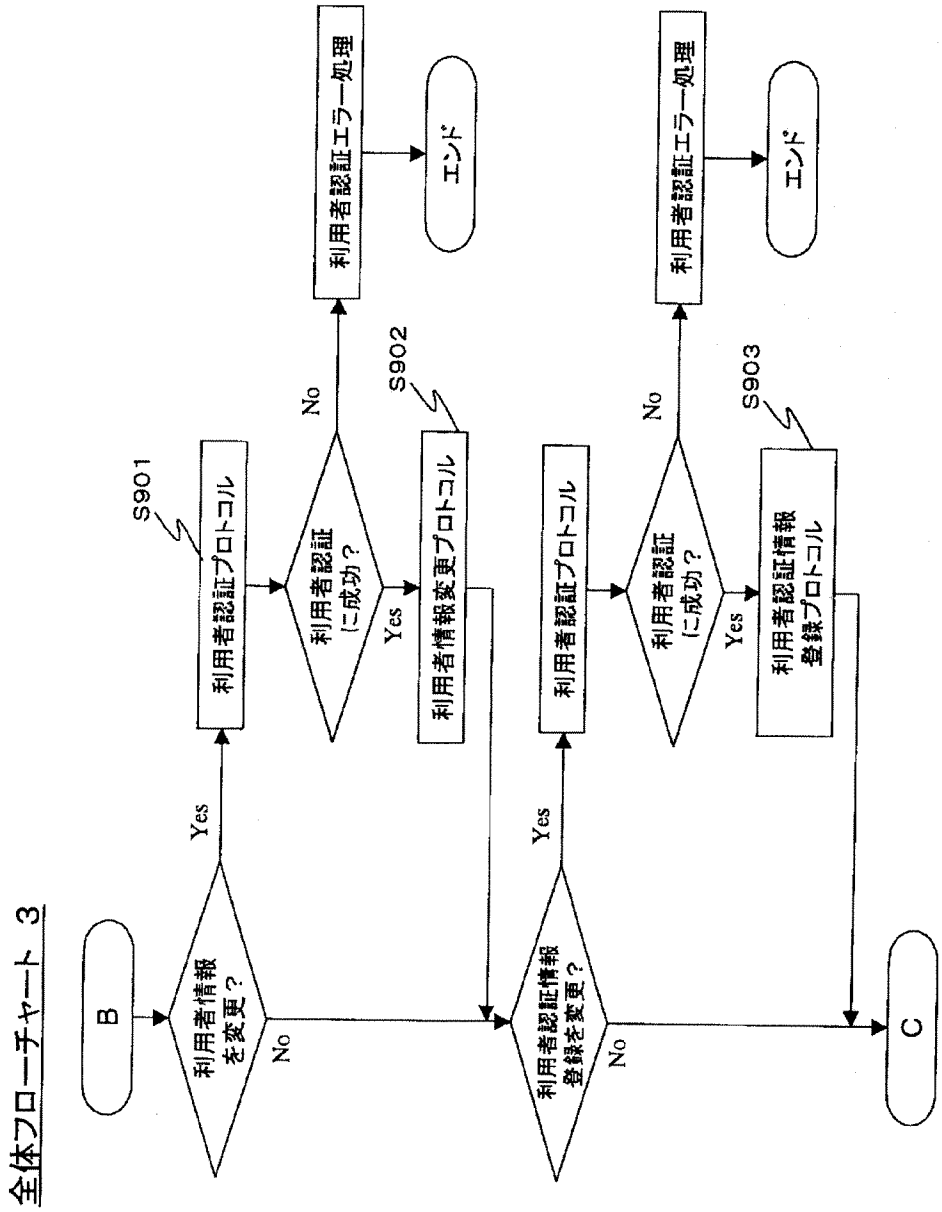

全体フローチャート　1
スタート
接続初回か？
Yes
No
S701
機器登録プロトコル
S702
機器認証プロトコル
機器認証
エラー？
Yes
No
機器認証エラー処理
エンド
A

【図８】

全体フローチャート　2

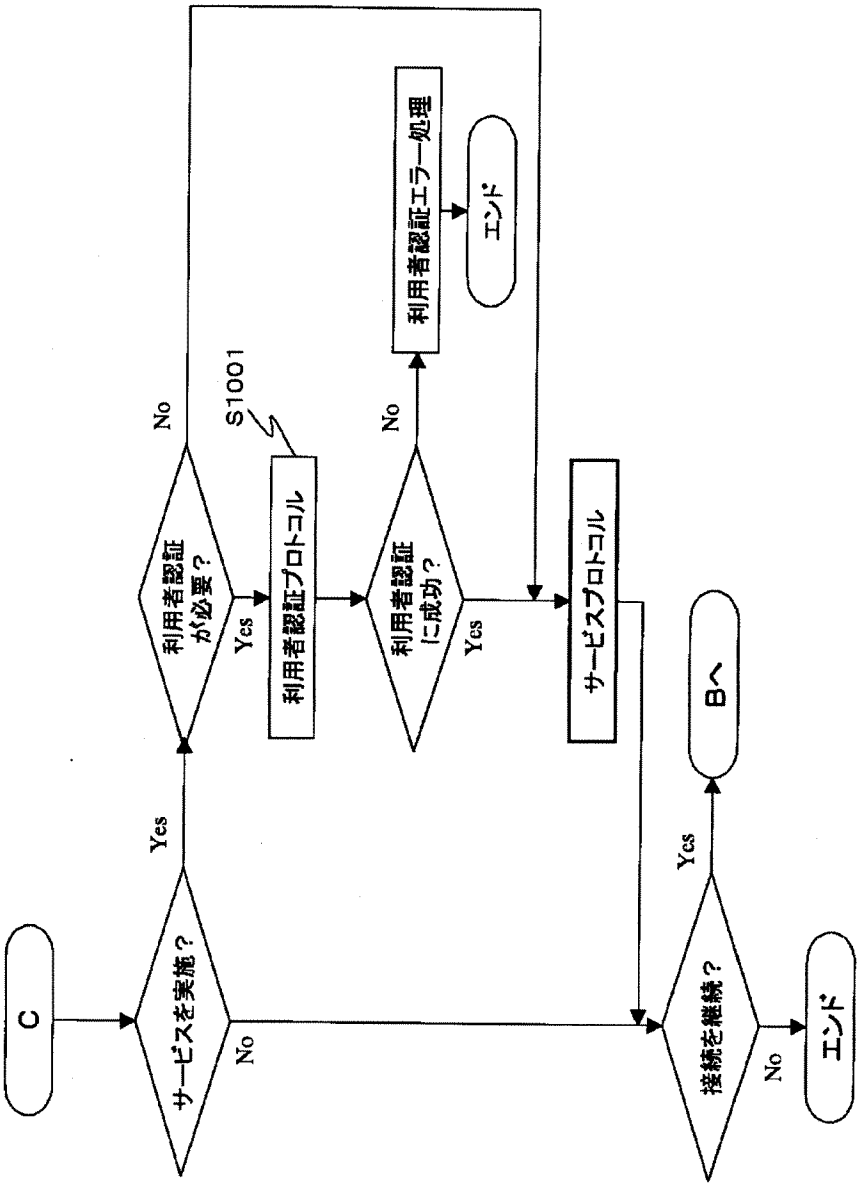


【図９】

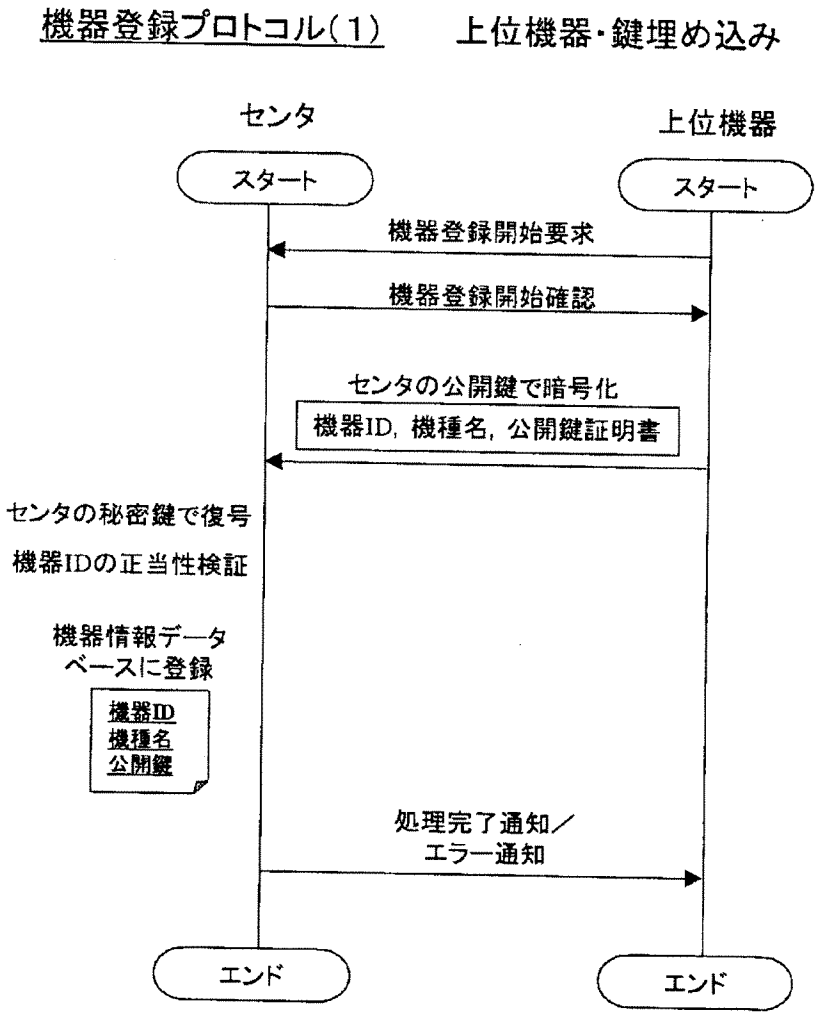

全体フローチャート 3
B
利用者情報を変更？
Yes
No
S901
利用者認証プロトコル
利用者認証に成功？
No
利用者認証エラー処理
エンド
Yes
S902
利用者情報変更プロトコル
利用者認証情報登録を変更？
Yes
No
S901
利用者認証プロトコル
利用者認証に成功？
No
利用者認証エラー処理
エンド
Yes
S903
利用者認証情報登録プロトコル
C

【図１０】

全体フローチャート 4

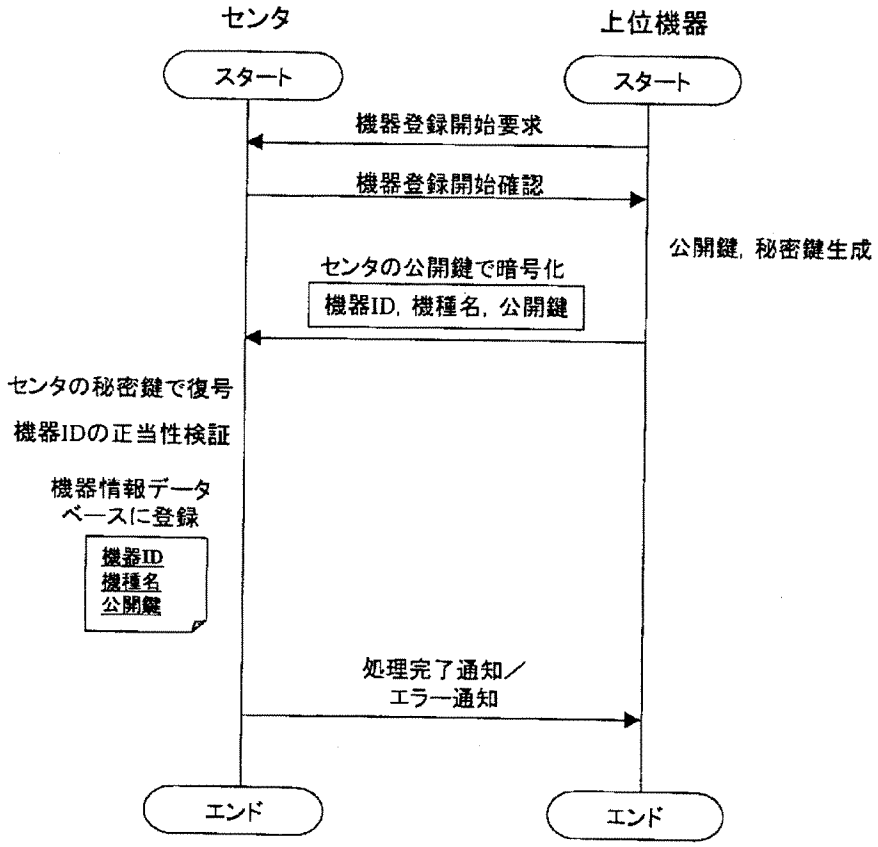


【図１１】


機器登録プロトコル(1)　上位機器・鍵埋め込み
センタ
上位機器
スタート
スタート
機器登録開始要求
機器登録開始確認
センタの公開鍵で暗号化
機器ID，機種名，公開鍵証明書
センタの秘密鍵で復号
機器IDの正当性検証
機器情報データベースに登録
機器ID
機種名
公開鍵
処理完了通知／エラー通知
エンド
エンド

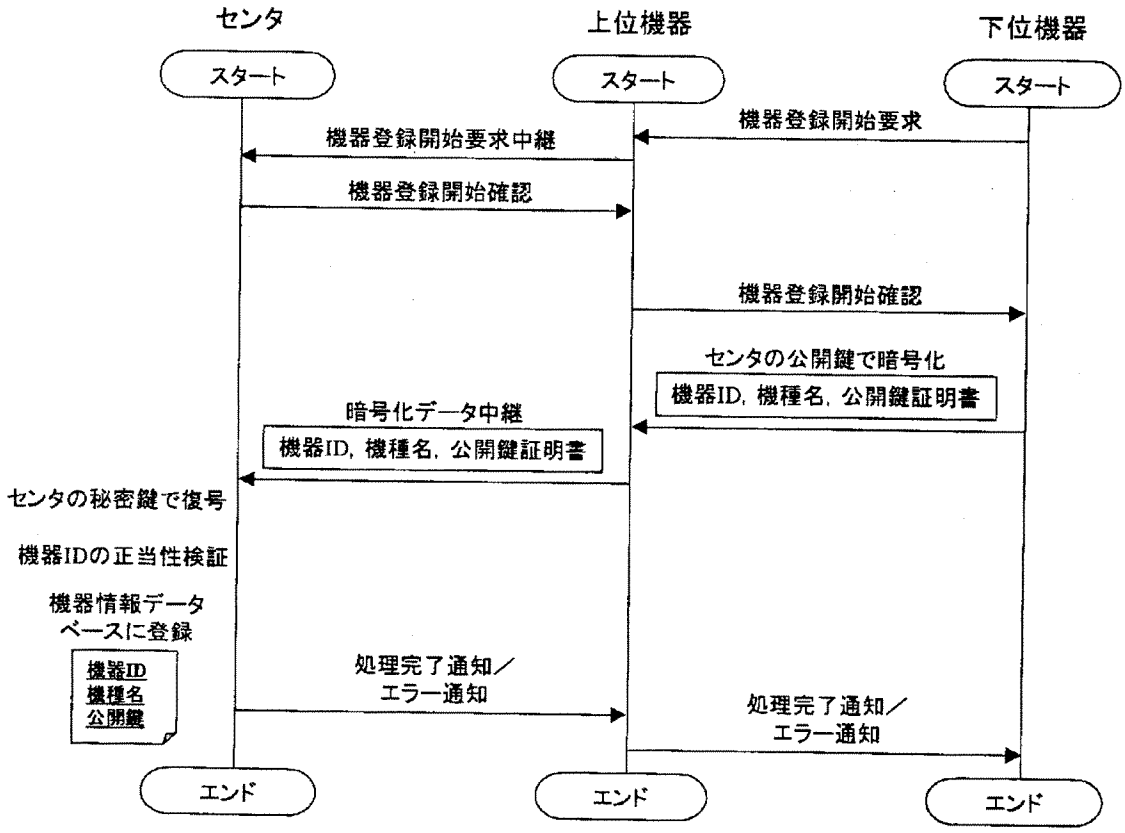
【図１２】

機器登録プロトコル(2)　　上位機器・鍵生成

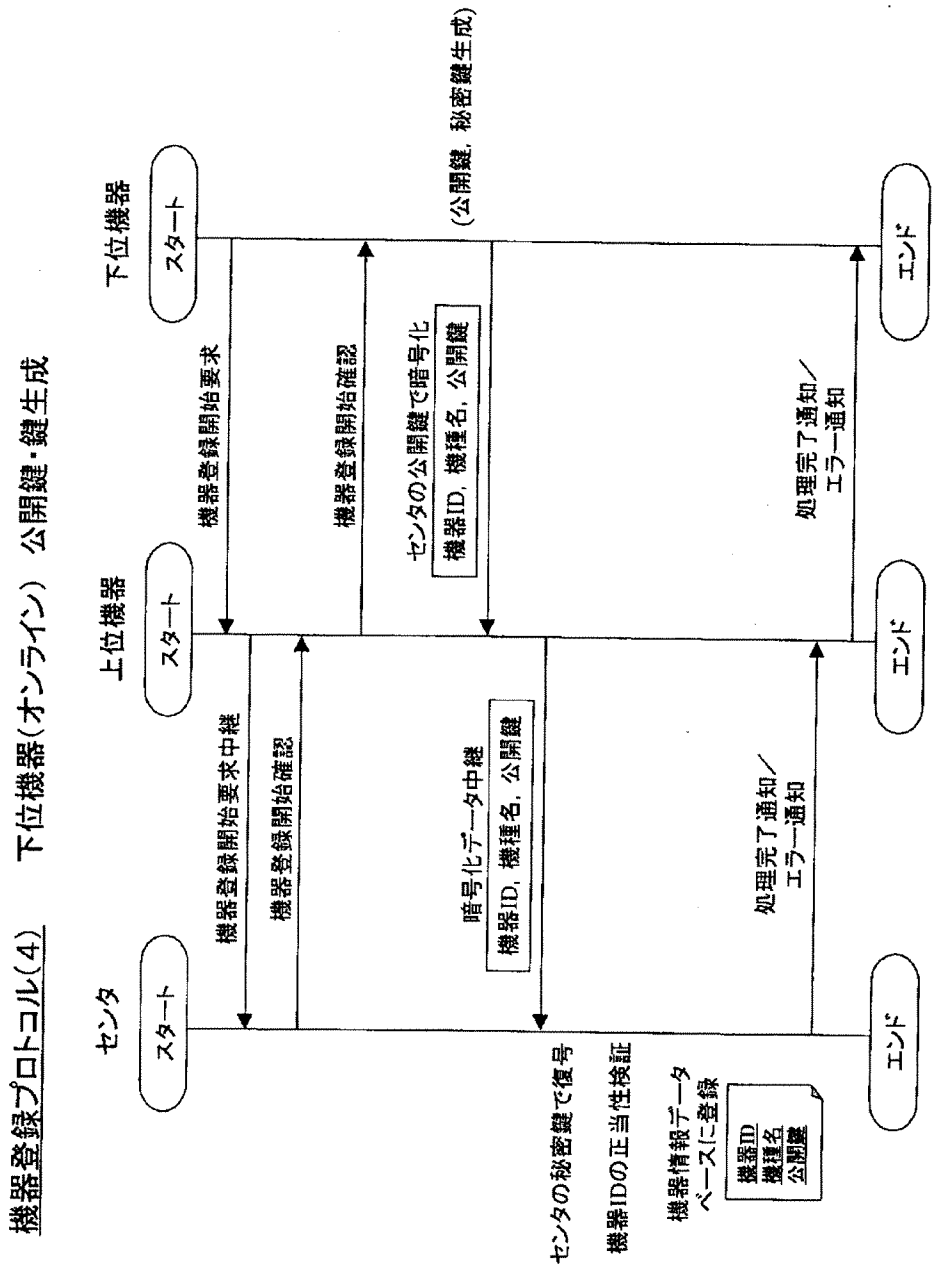


【図１３】

機器登録プロトコル(3)　　下位機器(オンライン)　公開鍵・鍵埋め込み

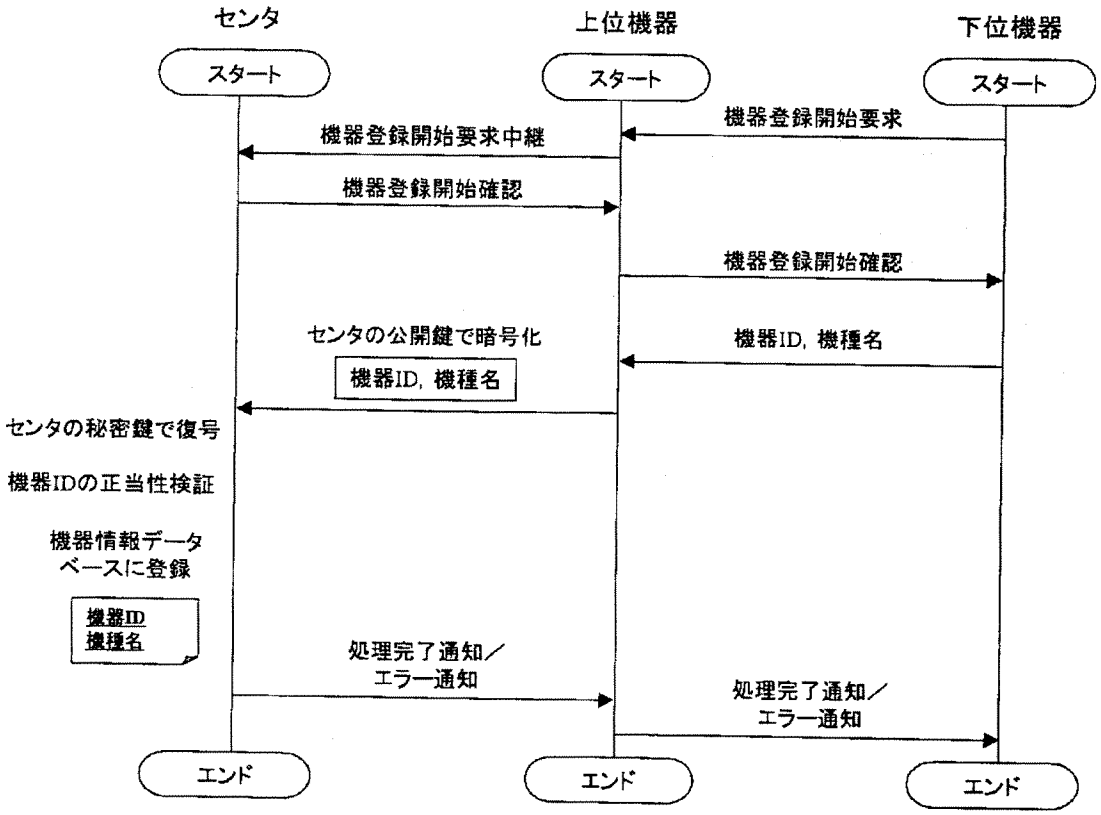


【図１４】


機器登録プロトコル(4)　下位機器(オンライン)　公開鍵・鍵生成
センタ
上位機器
下位機器
スタート
スタート
スタート
機器登録開始要求中継
機器登録開始確認
機器登録開始要求
機器登録開始確認
センタの公開鍵で暗号化
機器ID，機種名，公開鍵
(公開鍵，秘密鍵生成)
暗号化データ中継
機器ID，機種名，公開鍵
処理完了通知／
エラー通知
処理完了通知／
エラー通知
センタの秘密鍵で復号
機器IDの正当性検証
機器情報データ
ベースに登録
機器ID
機種名
公開鍵
エンド
エンド
エンド

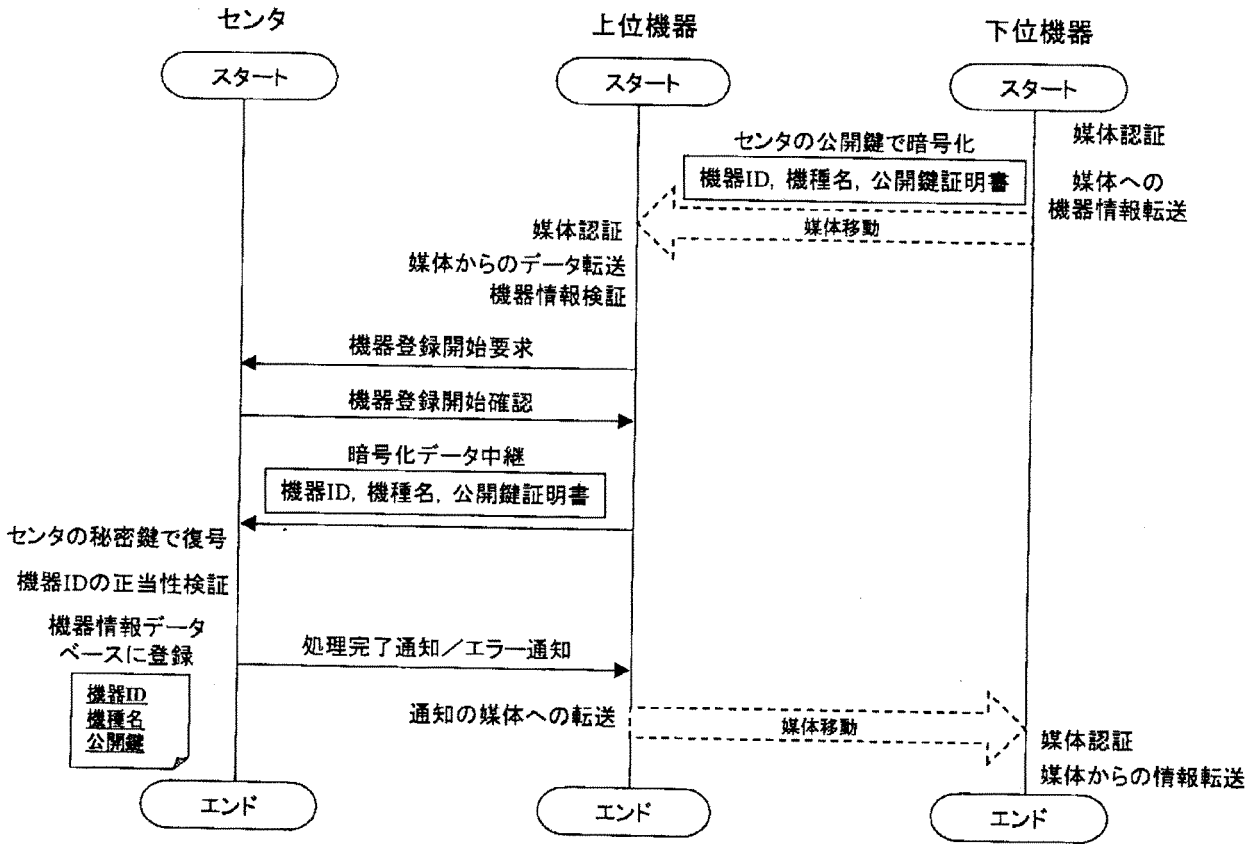
【図１５】

機器登録プロトコル(5)　　下位機器(オンライン) 共通鍵, 暗号化なし

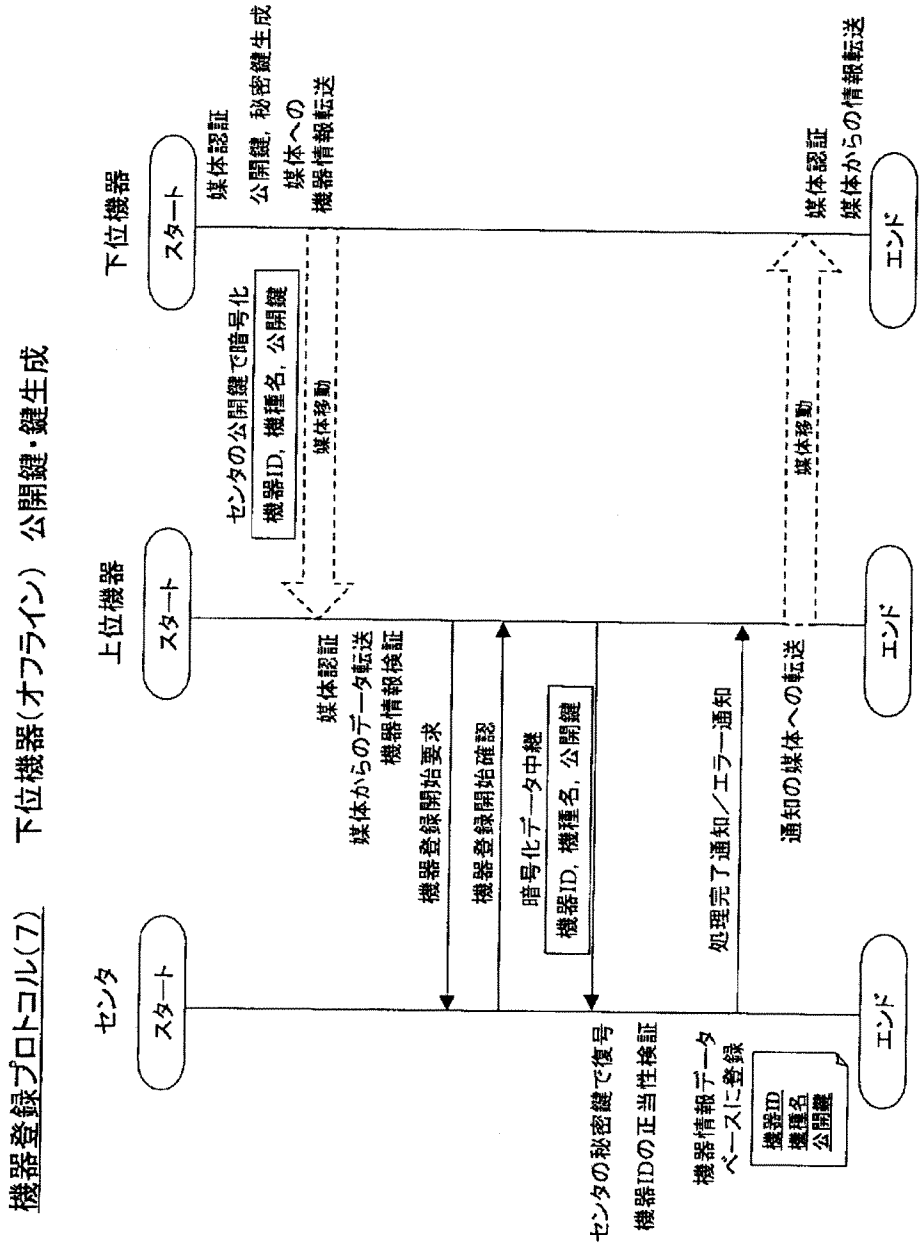


【図16】

機器登録プロトコル(6)　　下位機器(オフライン) 公開鍵・鍵埋め込み

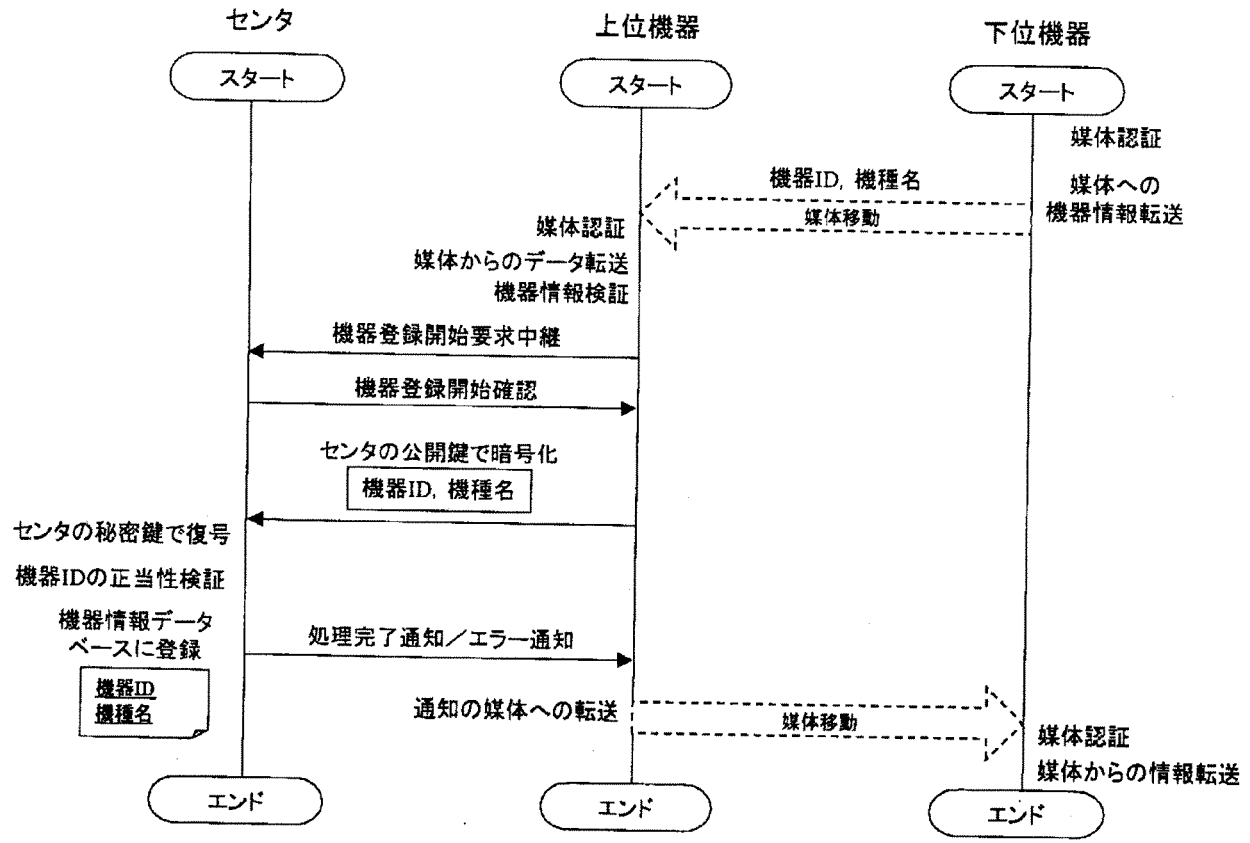


【図１７】


機器登録プロトコル(7)　下位機器(オフライン)　公開鍵・鍵生成
センタ
上位機器
下位機器
スタート
スタート
スタート
媒体認証
公開鍵，秘密鍵生成
媒体への
機器情報転送
センタの公開鍵で暗号化
機器ID，機種名，公開鍵
媒体移動
媒体認証
媒体からのデータ転送
機器情報検証
機器登録開始要求
機器登録開始確認
暗号化データ中継
機器ID，機種名，公開鍵
処理完了通知／エラー通知
通知の媒体への転送
媒体移動
媒体認証
媒体からの情報転送
センタの秘密鍵で復号
機器IDの正当性検証
機器情報データ
ベースに登録
機器ID
機種名
公開鍵
エンド
エンド
エンド

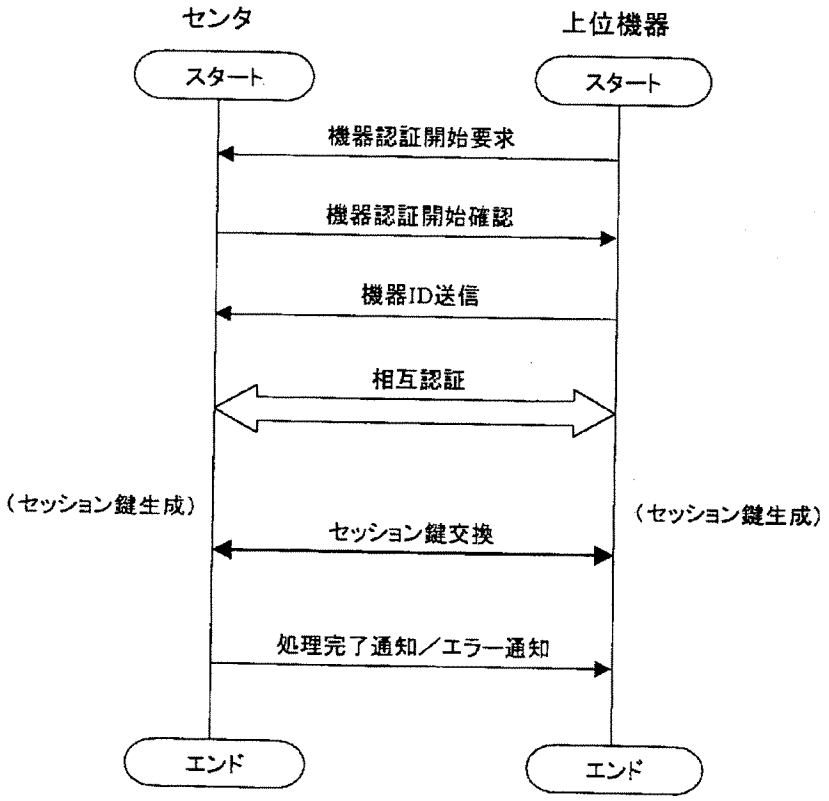
【図18】

機器登録プロトコル(8)　　下位機器(オフライン)　共通鍵，暗号化なし

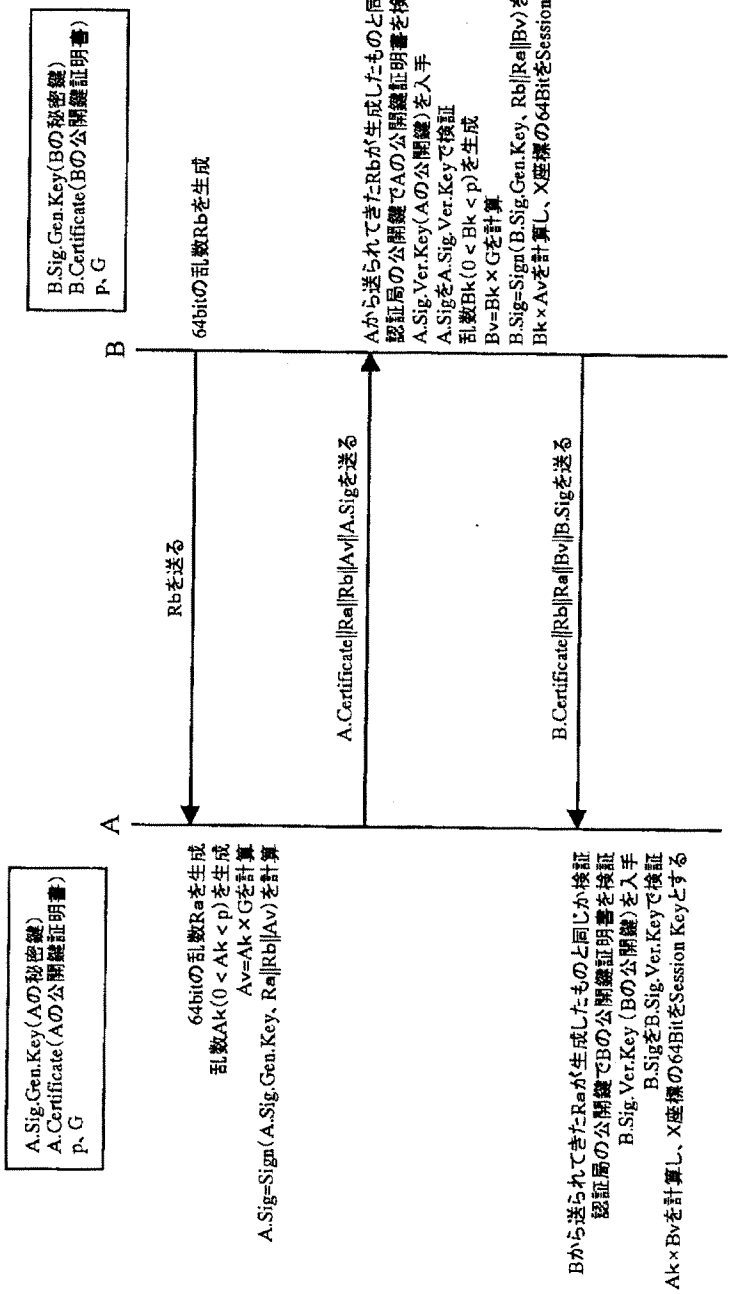


【図１９】

機器認証プロトコル(1)　　センター上位機器

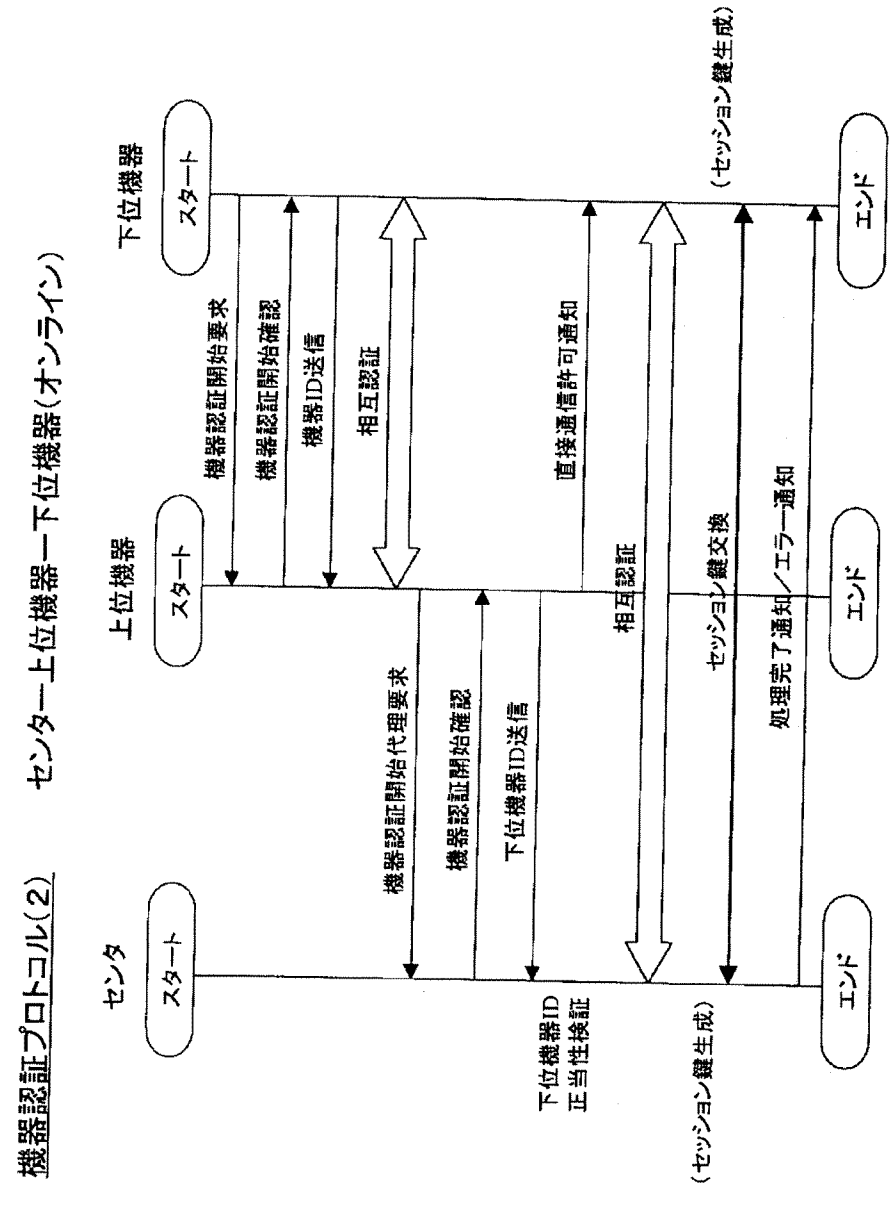


【図２０】

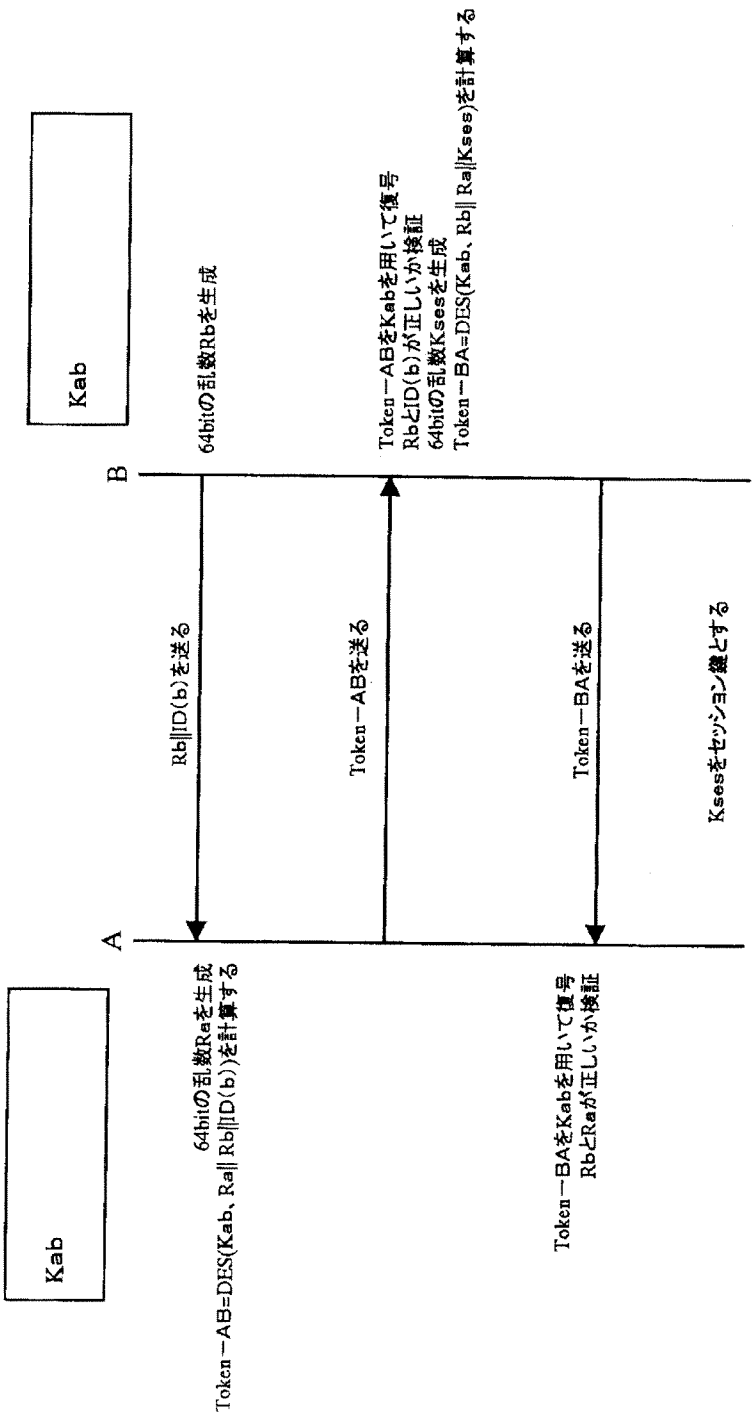


ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図２１】


機器認証プロトコル(2)　センター上位機器ー下位機器(オンライン)
センタ
上位機器
下位機器
スタート
スタート
スタート
エンド
エンド
エンド
機器認証開始要求
機器認証開始確認
機器ID送信
相互認証
直接通信許可通知
(セッション鍵生成)
機器認証開始代理要求
機器認証開始確認
下位機器ID送信
相互認証
セッション鍵交換
処理完了通知/エラー通知
下位機器ID
正当性検証
(セッション鍵生成)

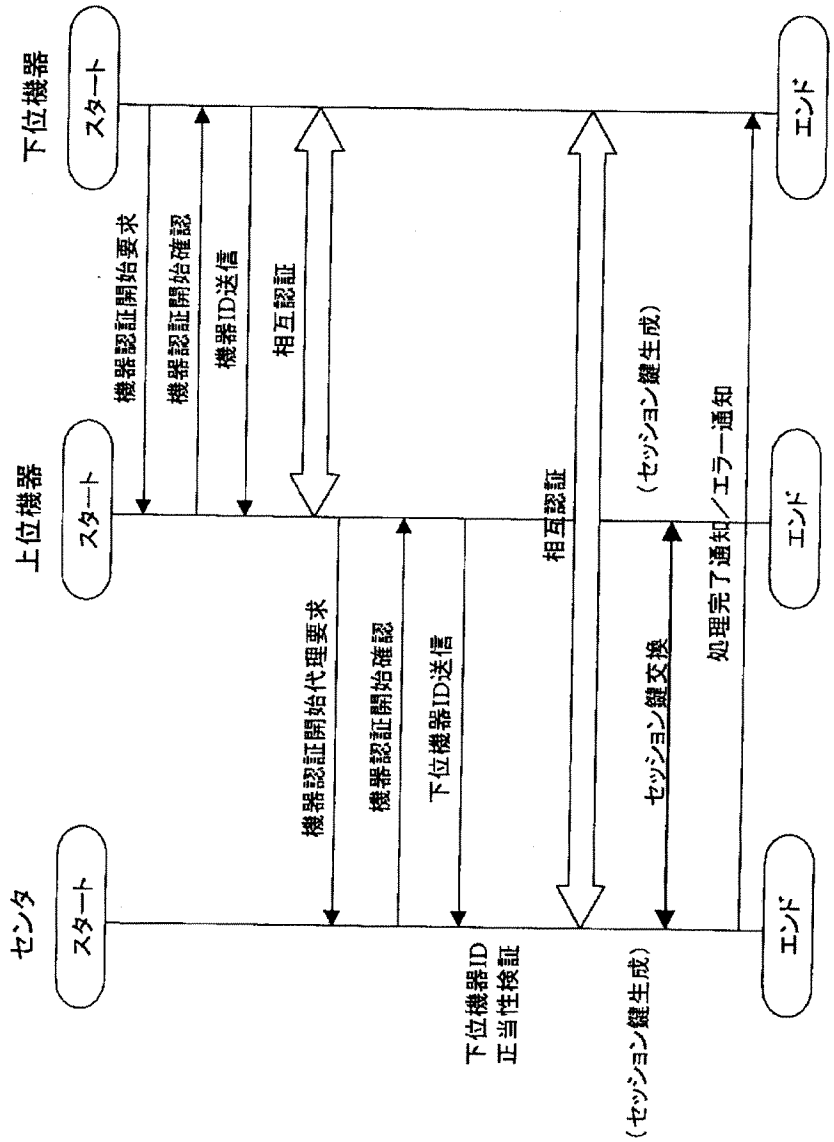
【図２２】



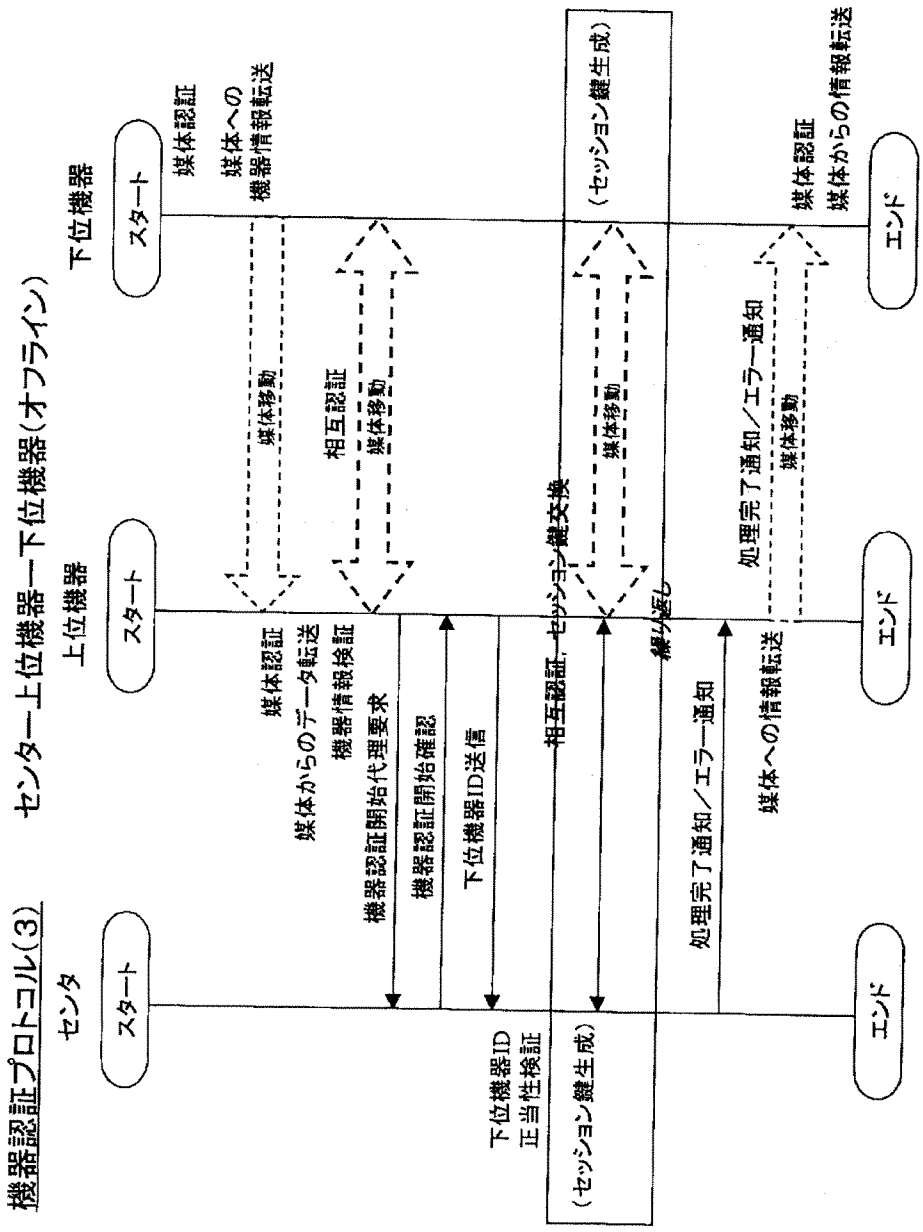
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図２３】

機器認証プロトコル(3)　センター上位機器－下位機器(オンライン／暗号化機能なし)

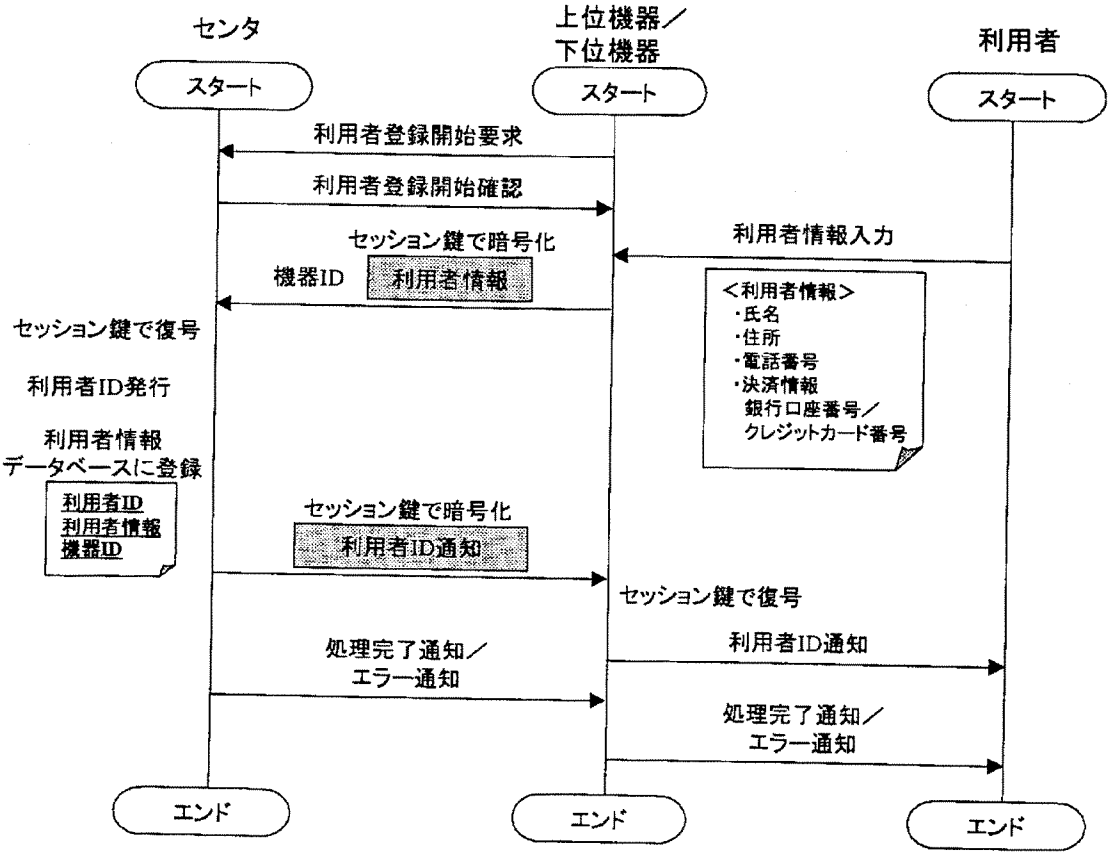


【図２４】

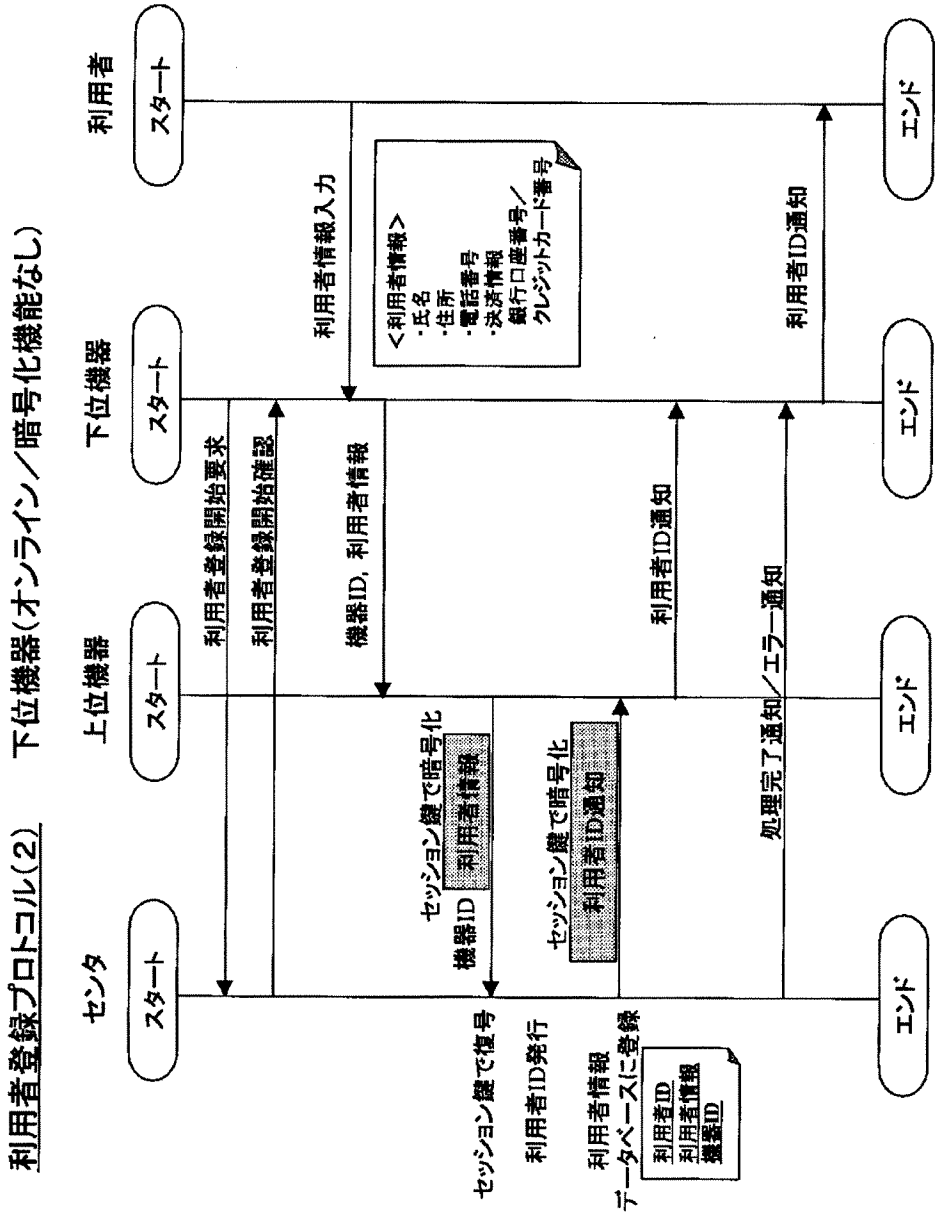

機器認証プロトコル(3)　センター上位機器－下位機器(オフライン)
センタ
上位機器
下位機器
スタート
媒体認証
媒体への
機器情報転送
媒体移動
相互認証
媒体移動
（セッション鍵生成）
媒体認証
媒体からの情報転送
エンド
媒体認証
媒体からのデータ転送
機器情報検証
機器認証開始代理要求
機器認証開始確認
下位機器ID送信
相互認証、セッション鍵交換
媒体移動
処理完了通知／エラー通知
媒体への情報転送
エンド
下位機器ID
正当性検証
（セッション鍵生成）
処理完了通知／エラー通知
媒体移動
エンド

【図２５】

利用者登録プロトコル(１)　　上位機器，下位機器(オンライン)

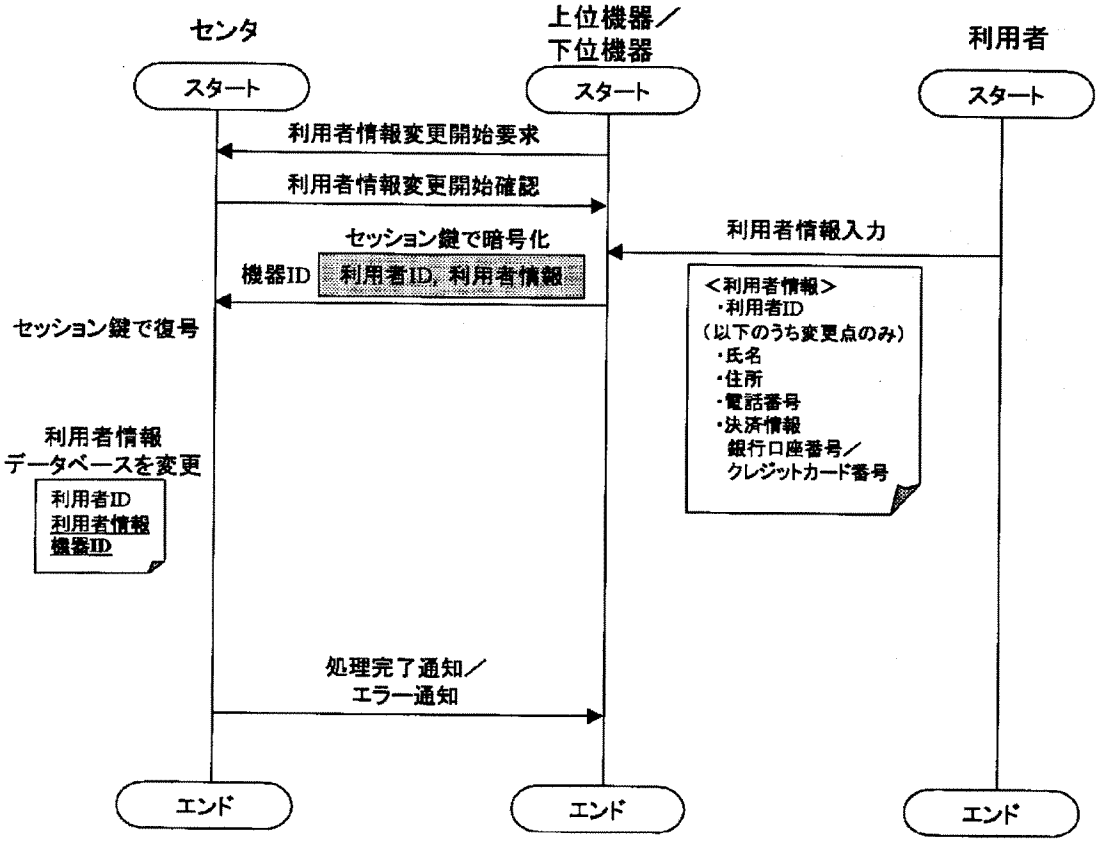


【図２６】

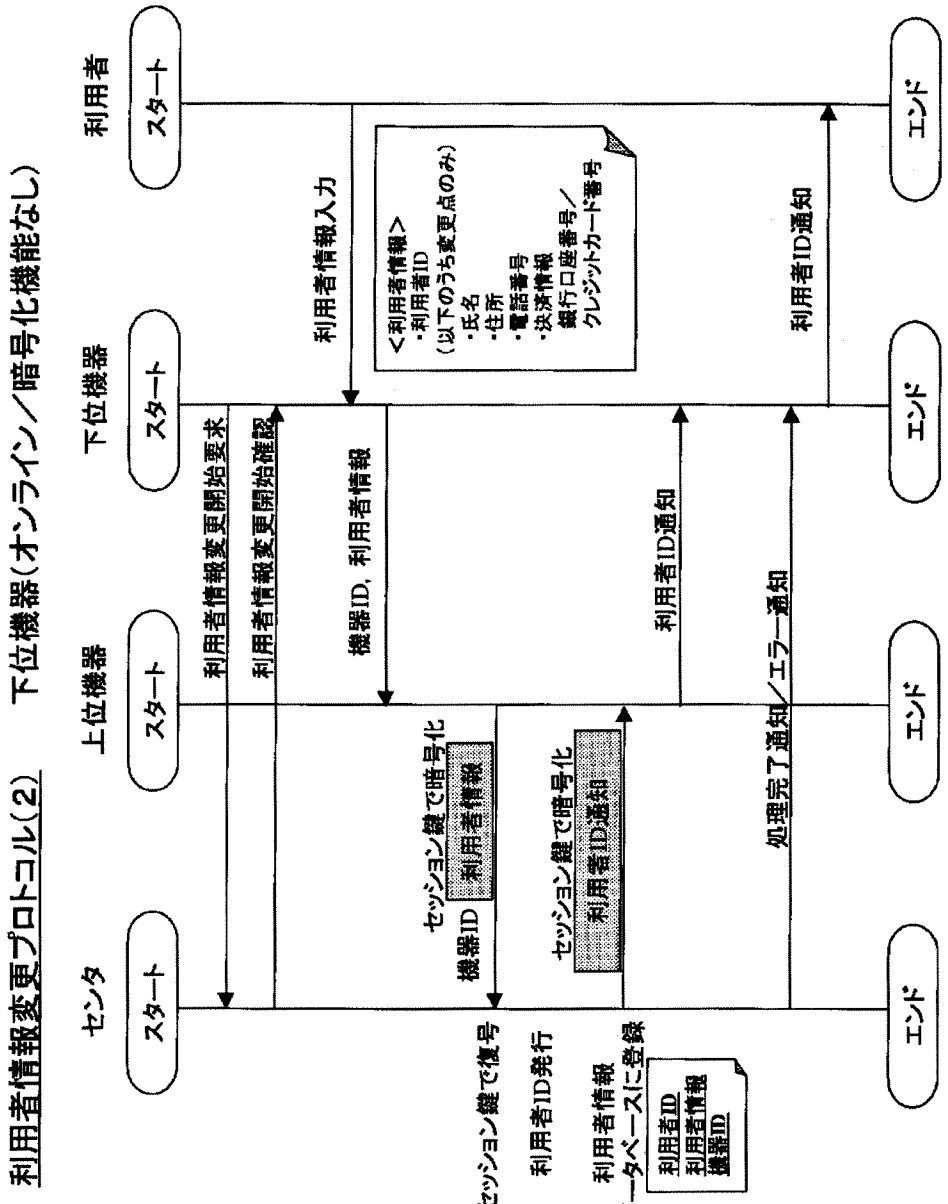

利用者登録プロトコル(2)　下位機器(オンライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
エンド
利用者登録開始要求
利用者登録開始確認
機器ID, 利用者情報
利用者情報入力
<利用者情報>
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
セッション鍵で暗号化
利用者情報
機器ID
セッション鍵で復号
利用者ID発行
セッション鍵で暗号化
利用者ID通知
利用者ID通知
処理完了通知／エラー通知
利用者ID通知
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID

【図２７】

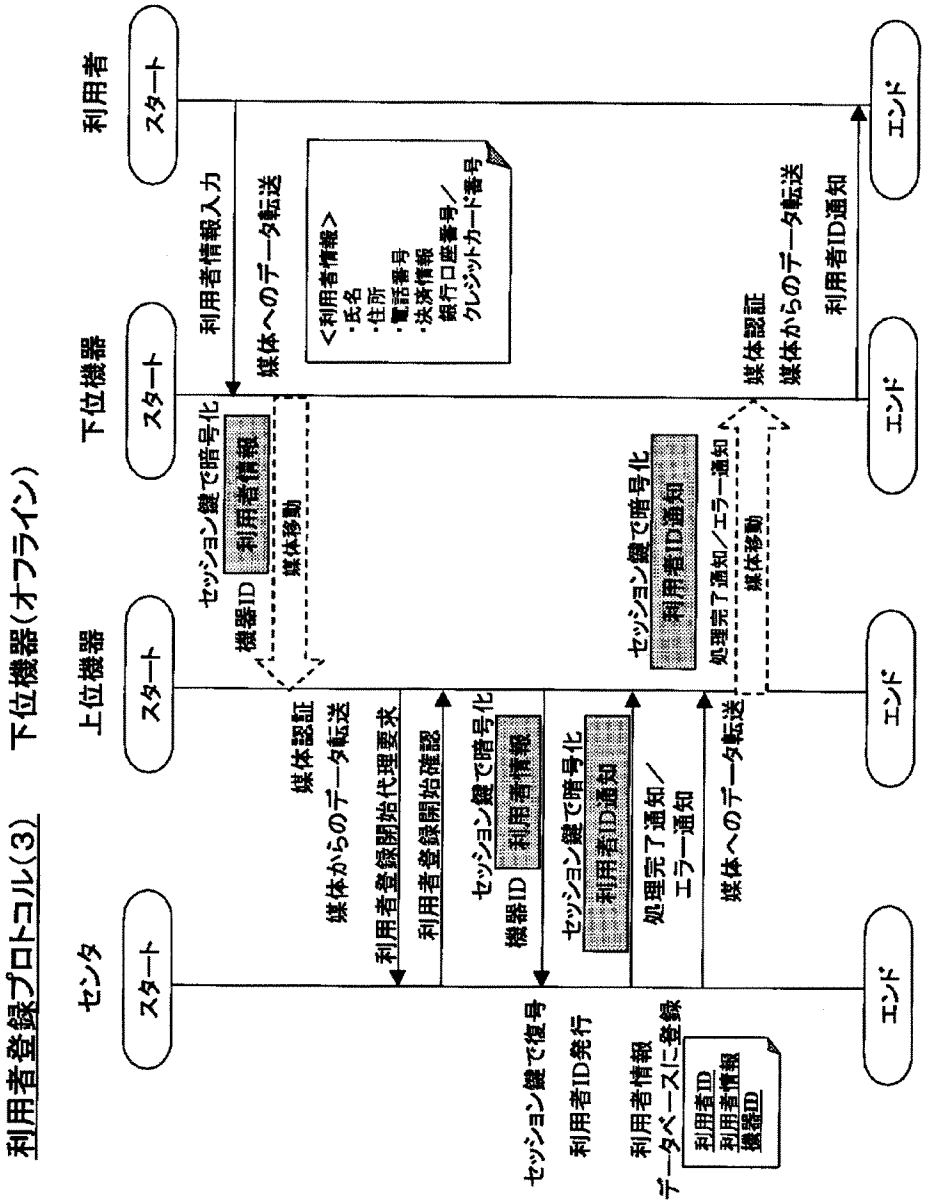
利用者情報変更プロトコル(1)　　上位機器，下位機器(オンライン)



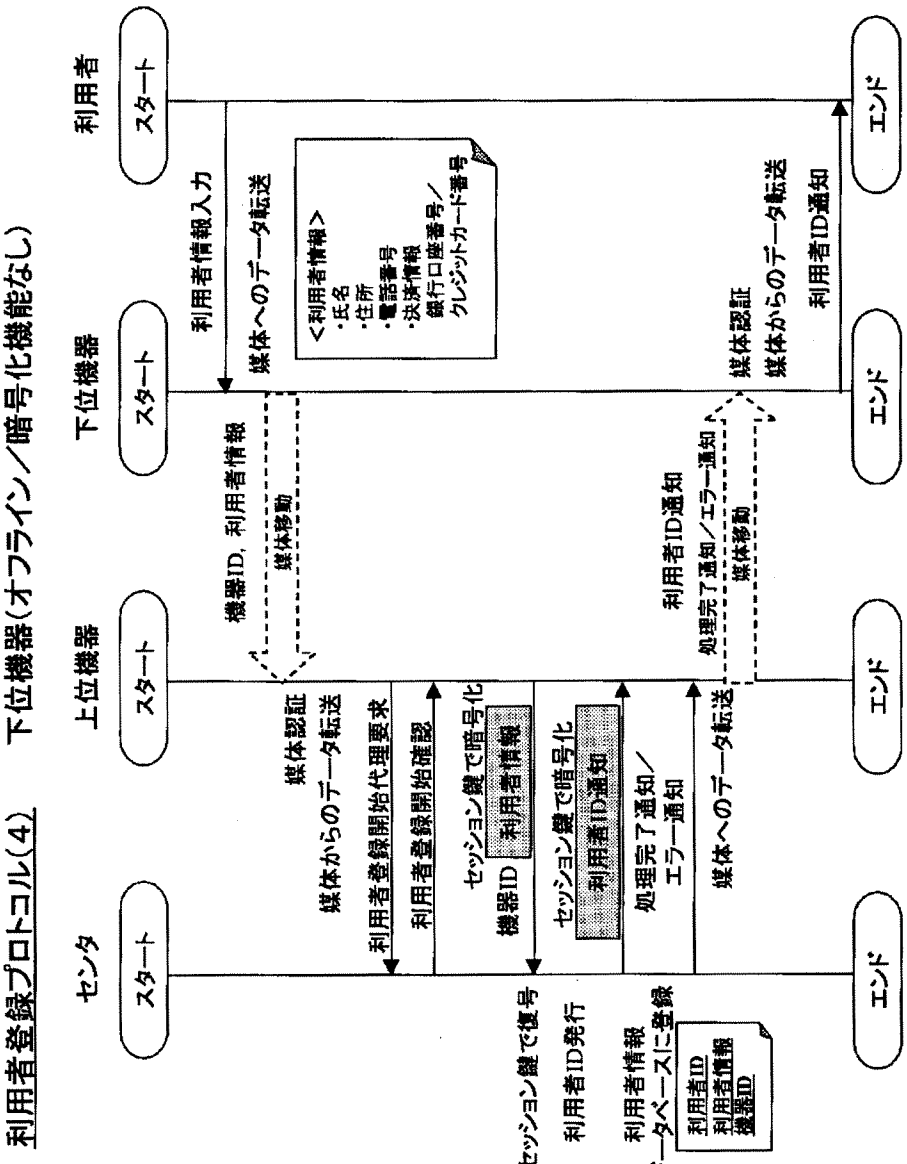
【図２８】


利用者情報変更プロトコル(2)　下位機器(オンライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
利用者情報変更開始要求
利用者情報変更開始確認
利用者情報入力
<利用者情報>
・利用者ID
(以下のうち変更点のみ)
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
機器ID, 利用者情報
セッション鍵で暗号化
機器ID
利用者情報
セッション鍵で復号
利用者ID発行
セッション鍵で暗号化
利用者ID通知
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID
利用者ID通知
処理完了通知／エラー通知
利用者ID通知
エンド

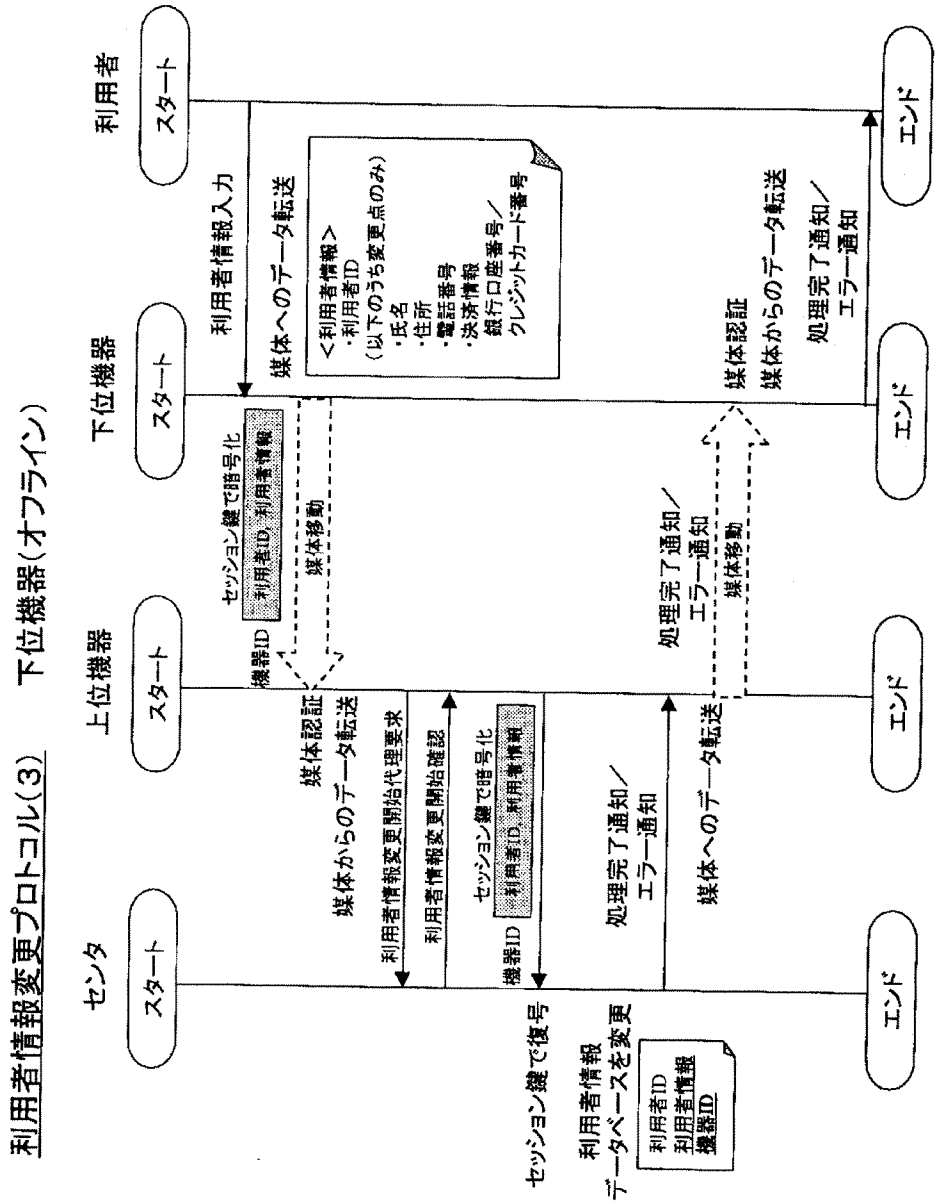
【図２９】


利用者登録プロトコル(3)　下位機器(オフライン)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
利用者情報入力
媒体へのデータ転送
<利用者情報>
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
セッション鍵で暗号化
機器ID
利用者情報
媒体移動
媒体認証
媒体からのデータ転送
利用者登録開始代理要求
利用者登録開始確認
セッション鍵で暗号化
機器ID
利用者情報
セッション鍵で暗号化
利用者ID通知
セッション鍵で暗号化
利用者ID通知
処理完了通知／
エラー通知
媒体へのデータ転送
処理完了通知／エラー通知
媒体移動
媒体認証
媒体からのデータ転送
利用者ID通知
セッション鍵で復号
利用者ID発行
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID
エンド
エンド
エンド
エンド

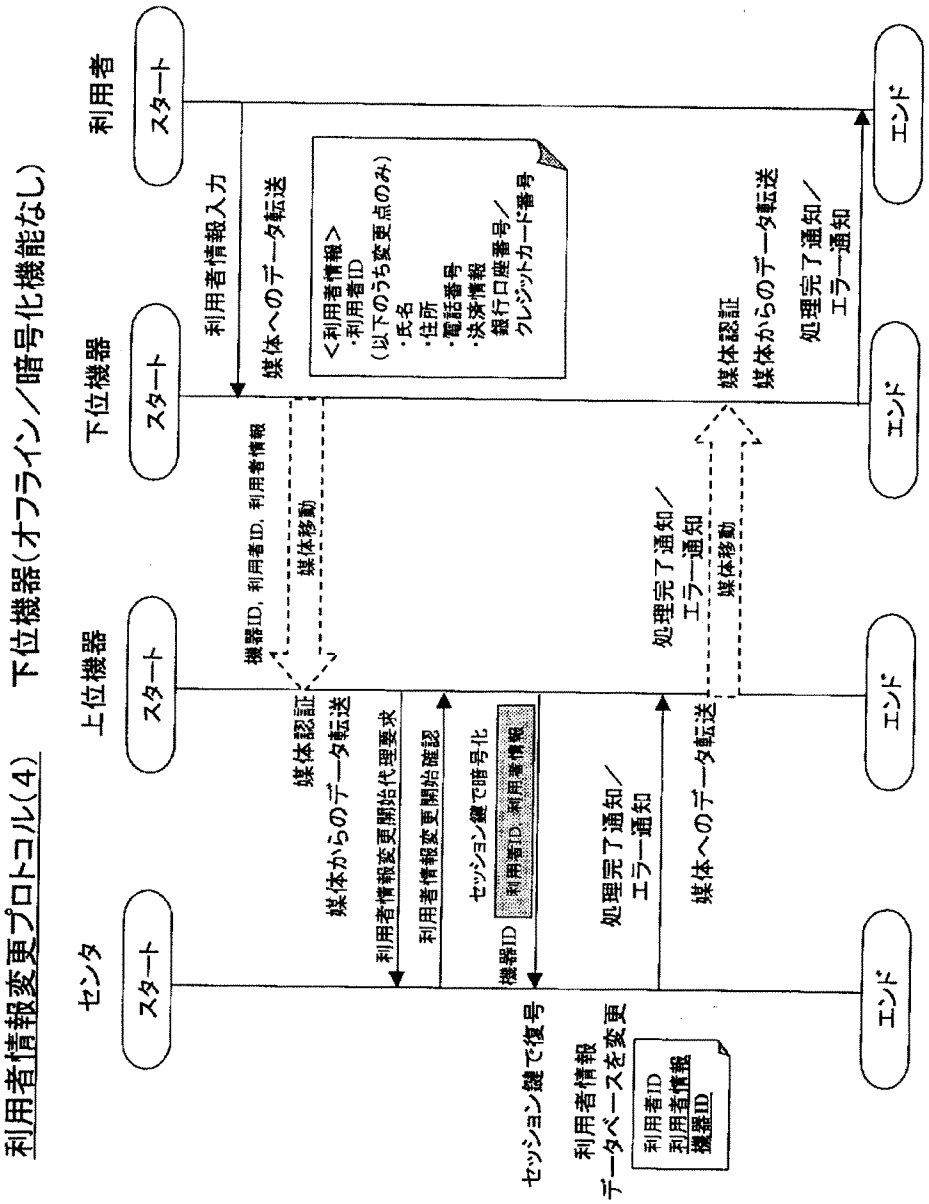
【図３０】


利用者登録プロトコル(4)　下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
利用者情報入力
媒体へのデータ転送
<利用者情報>
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
機器ID，利用者情報
媒体移動
媒体認証
媒体からのデータ転送
利用者登録開始代理要求
利用者登録開始確認
セッション鍵で暗号化
機器ID
利用者情報
セッション鍵で暗号化
利用者ID通知
処理完了通知／
エラー通知
媒体へのデータ転送
利用者ID通知
処理完了通知／エラー通知
媒体移動
媒体認証
媒体からのデータ転送
利用者ID通知
エンド
セッション鍵で復号
利用者ID発行
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID

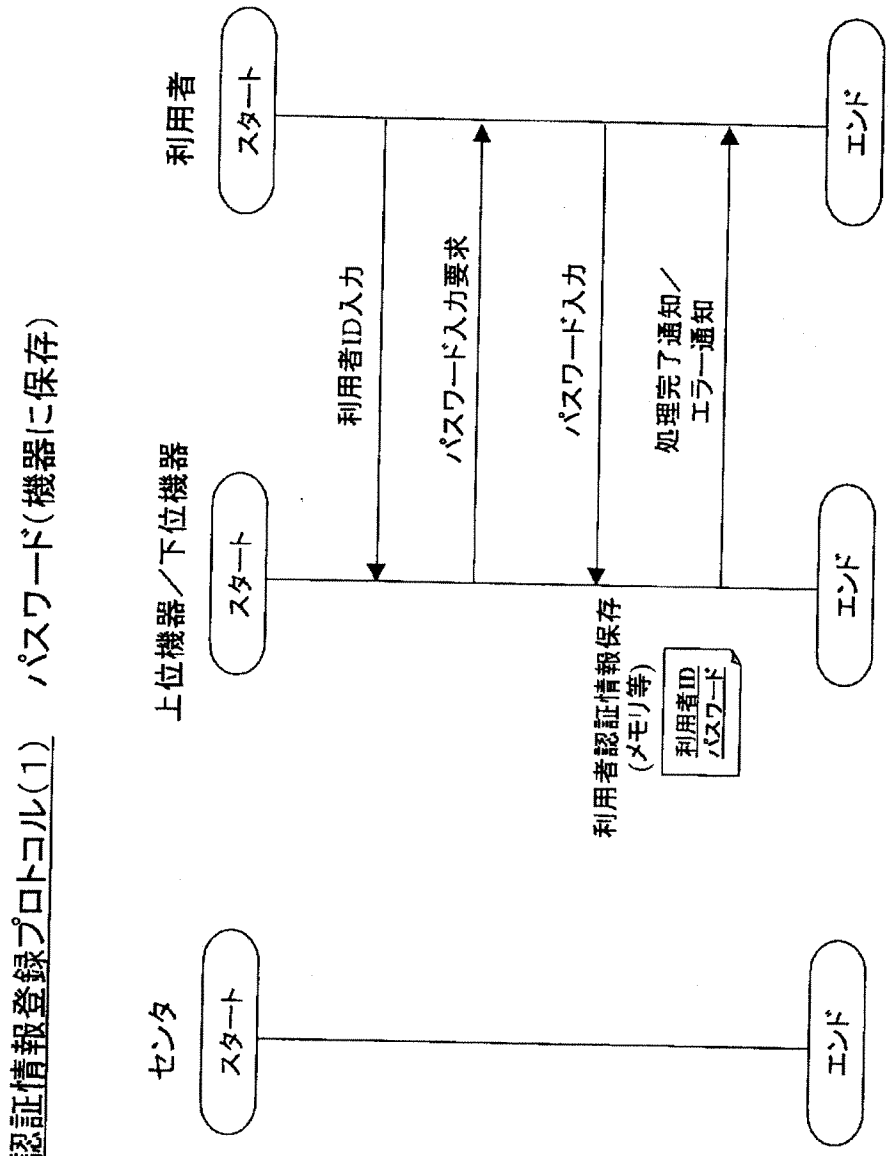
【図３１】


利用者情報変更プロトコル(3)　下位機器(オフライン)
センタ
上位機器
下位機器
利用者
スタート
エンド
利用者情報入力
媒体へのデータ転送
<利用者情報>
・利用者ID
(以下のうち変更点のみ)
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
セッション鍵で暗号化
利用者ID 利用者情報
機器ID
媒体移動
媒体認証
媒体からのデータ転送
利用者情報変更開始代理要求
利用者情報変更開始確認
セッション鍵で暗号化
利用者ID 利用者情報
機器ID
処理完了通知／
エラー通知
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
処理完了通知／
エラー通知
セッション鍵で復号
利用者情報
データベースを変更
利用者ID
利用者情報
機器ID

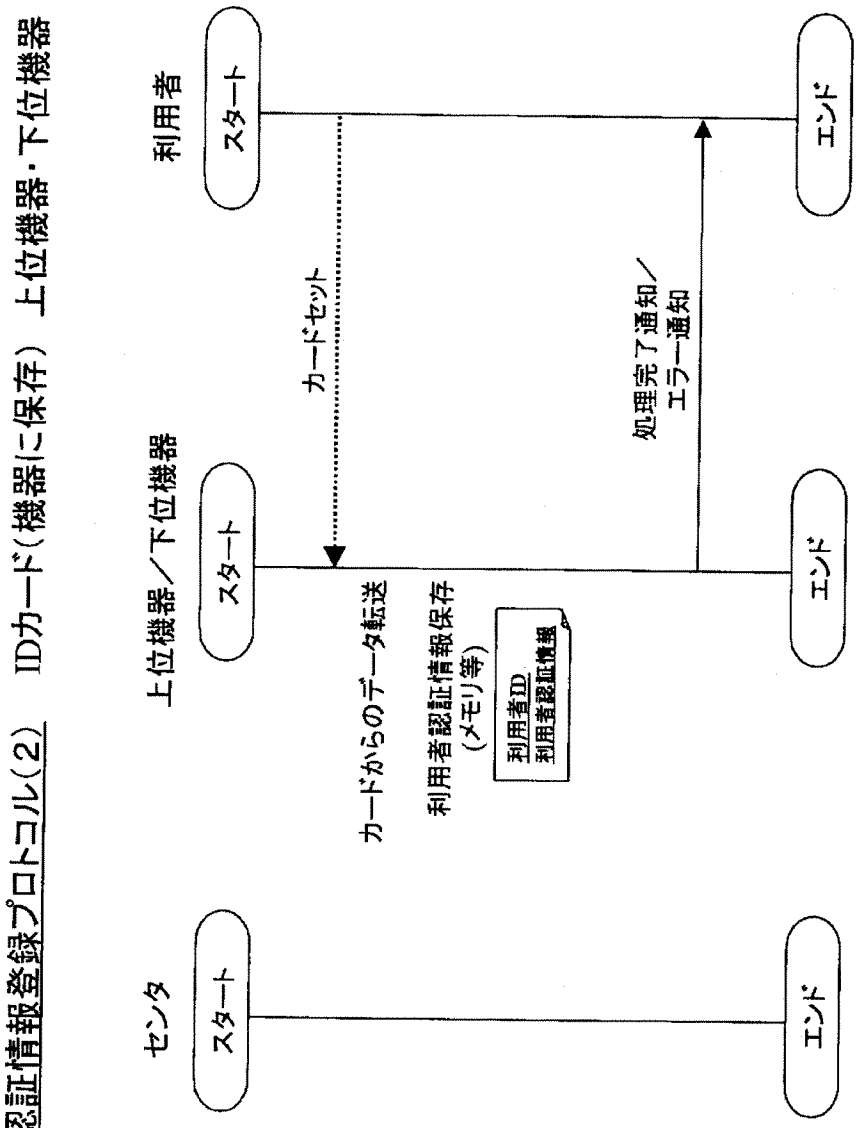
【図３２】


利用者情報変更プロトコル(4)　下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
利用者情報入力
媒体へのデータ転送
<利用者情報>
・利用者ID
(以下のうち変更点のみ)
・氏名
・住所
・電話番号
・決済情報
銀行口座番号／
クレジットカード番号
機器ID，利用者ID，利用者情報
媒体移動
媒体認証
媒体からのデータ転送
利用者情報変更開始代理要求
利用者情報変更開始確認
セッション鍵で暗号化
機器ID
利用者ID　利用者情報
処理完了通知／
エラー通知
媒体移動
媒体認証
媒体からのデータ転送
処理完了通知／
エラー通知
セッション鍵で復号
利用者情報
データベースを変更
利用者ID
利用者情報
機器ID
処理完了通知／
エラー通知
媒体へのデータ転送
エンド
エンド
エンド
エンド

【図３３】

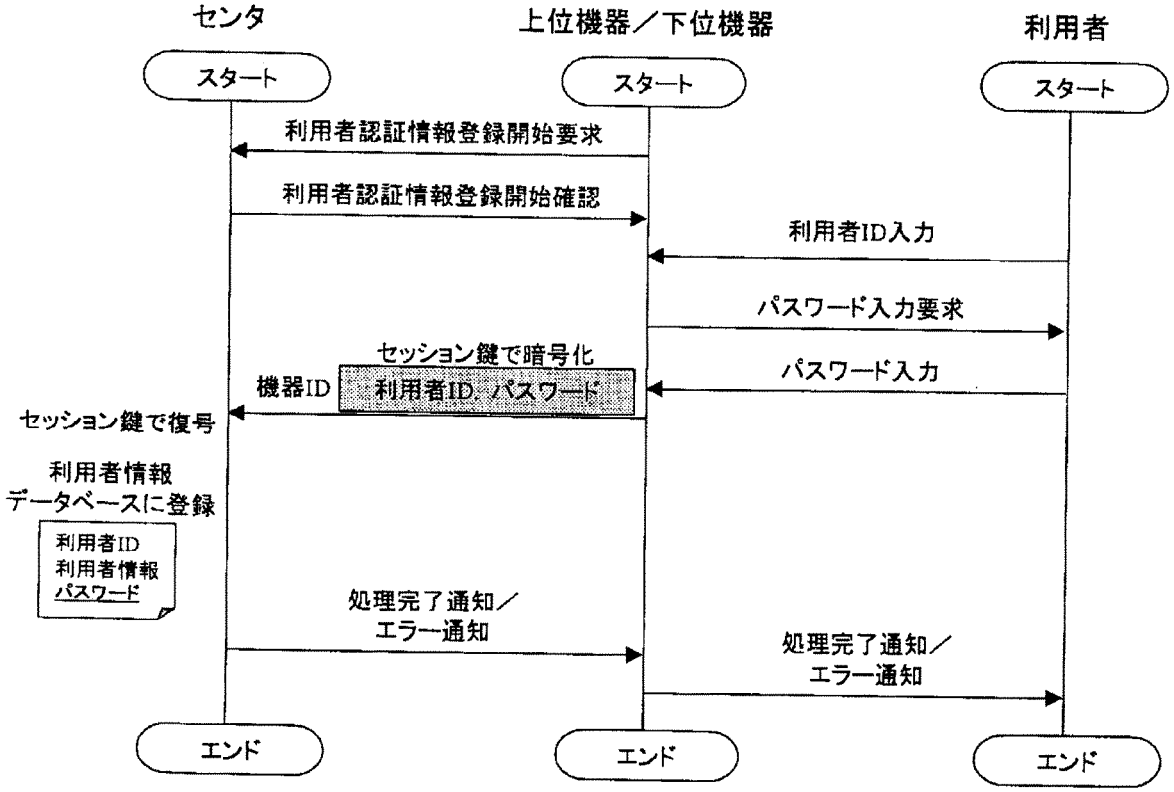

利用者認証情報登録プロトコル(1)　パスワード(機器に保存)
センタ
上位機器／下位機器
利用者
スタート
スタート
スタート
利用者ID入力
パスワード入力要求
パスワード入力
処理完了通知／
エラー通知
利用者認証情報保存
(メモリ等)
利用者ID
パスワード
エンド
エンド
エンド

【図３４】

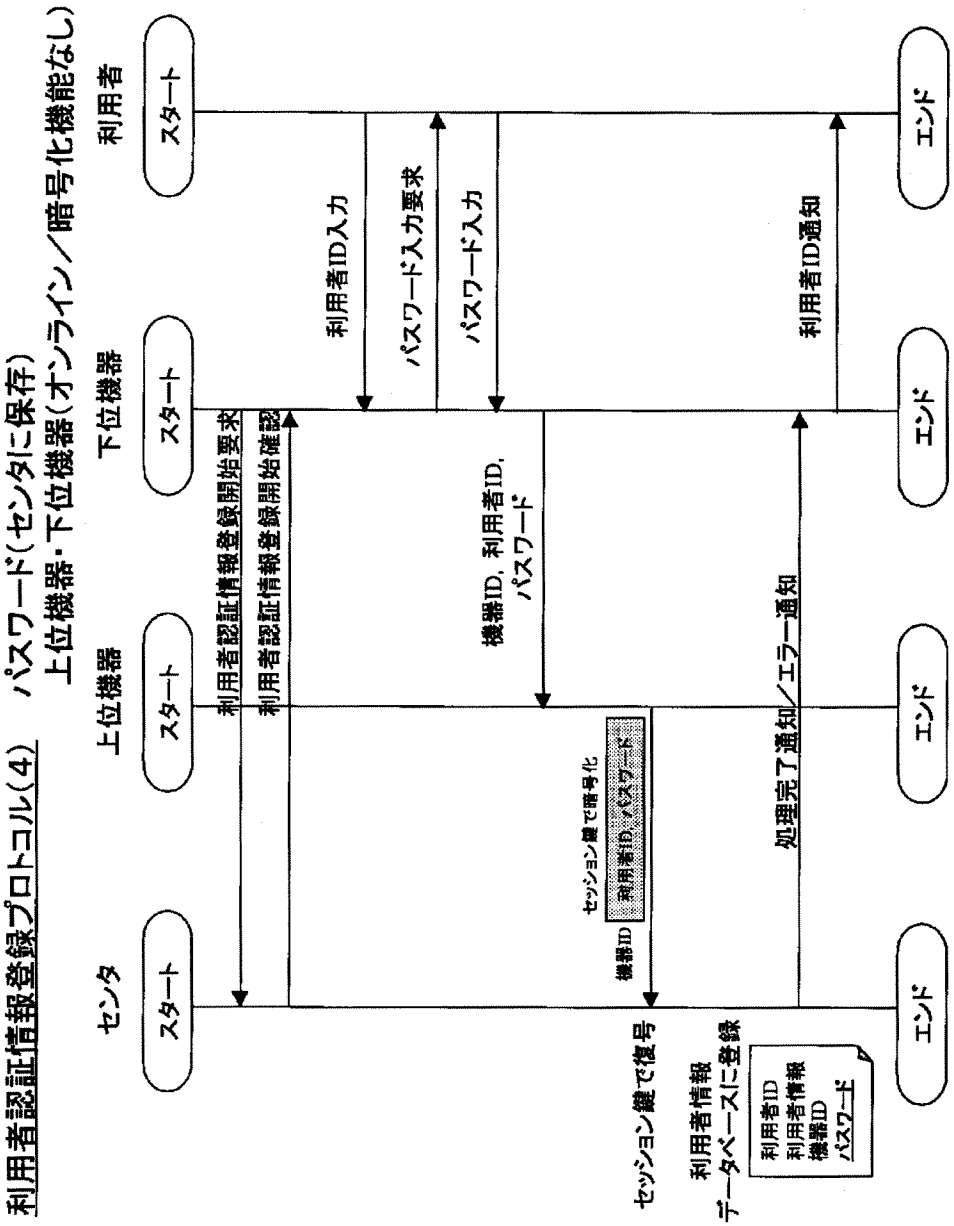

利用者認証情報登録プロトコル(2)　IDカード(機器に保存)　上位機器・下位機器
センタ
上位機器／下位機器
利用者
スタート
スタート
スタート
エンド
エンド
エンド
カードセット
カードからのデータ転送
利用者認証情報保存
(メモリ等)
利用者ID
利用者認証情報
処理完了通知／
エラー通知

【図35】

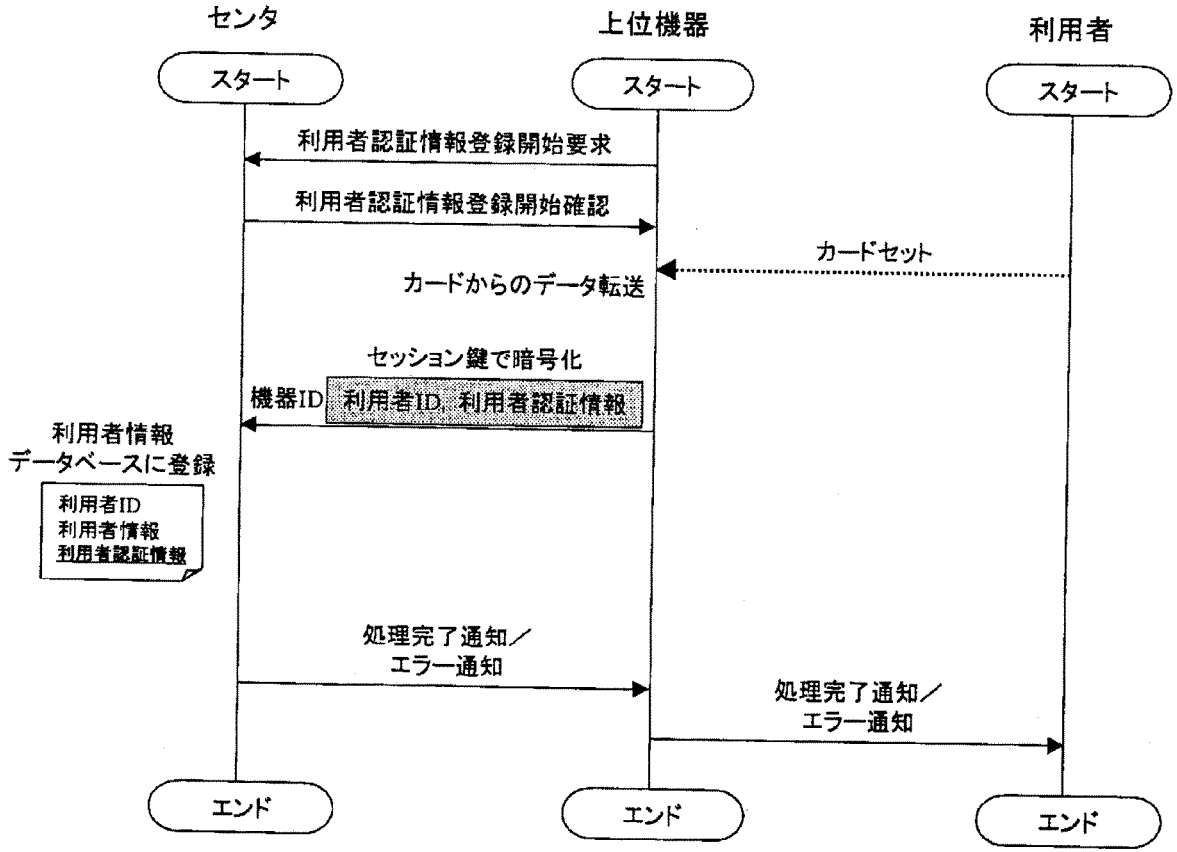
利用者認証情報登録プロトコル(3)　パスワード(センタに保存)　上位機器・下位機器(オンライン



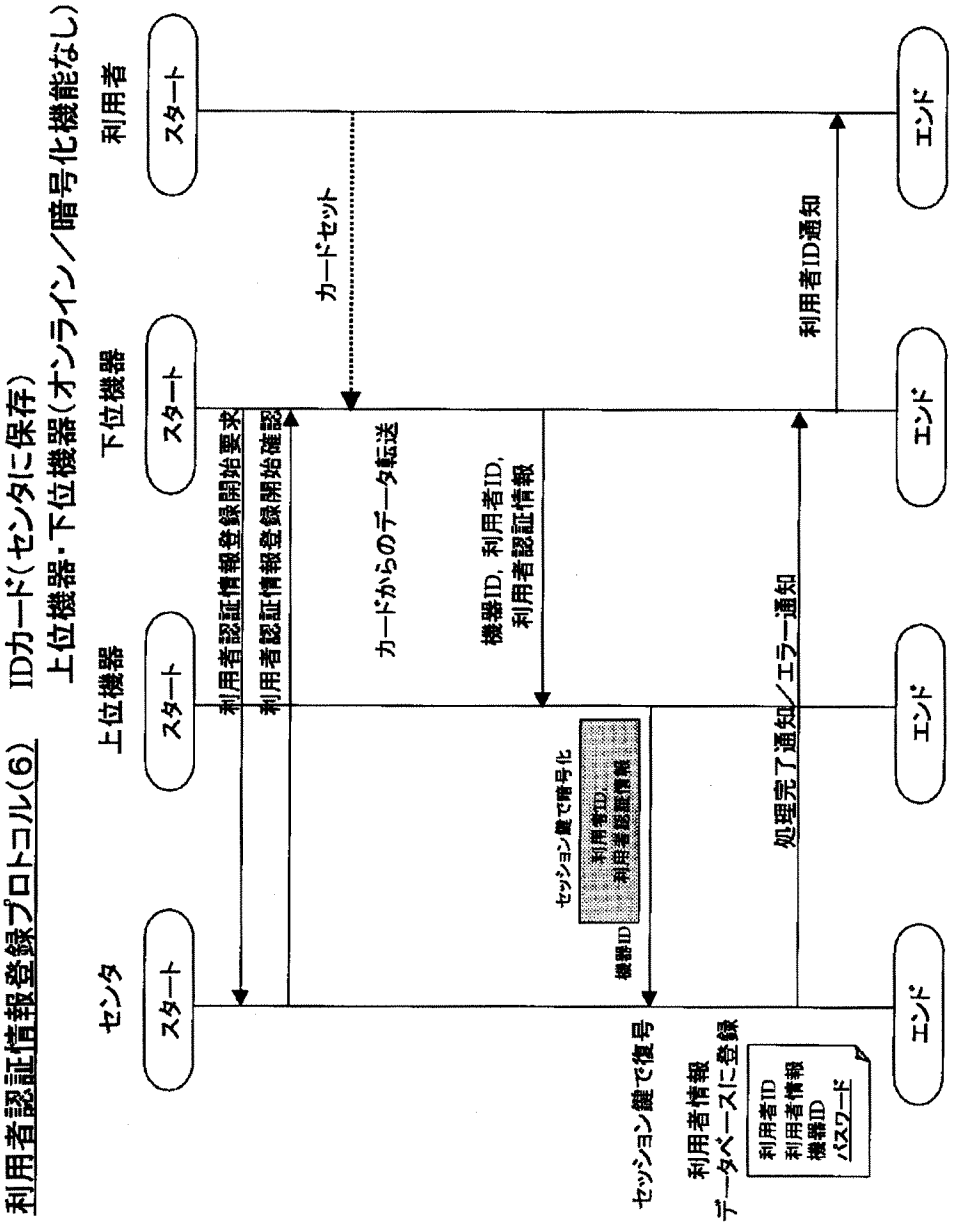
【図３６】


利用者認証情報登録プロトコル(4)　パスワード(センタに保存)
上位機器・下位機器(オンライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
エンド
利用者認証情報登録開始要求
利用者認証情報登録開始確認
利用者ID入力
パスワード入力要求
パスワード入力
機器ID, 利用者ID,
パスワード
セッション鍵で暗号化
利用者ID, パスワード
機器ID
処理完了通知／エラー通知
利用者ID通知
セッション鍵で復号
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID
パスワード

利用者認証情報登録プロトコル(5)　IDカード(センタに保存)　上位機器・下位機器(オンライン)

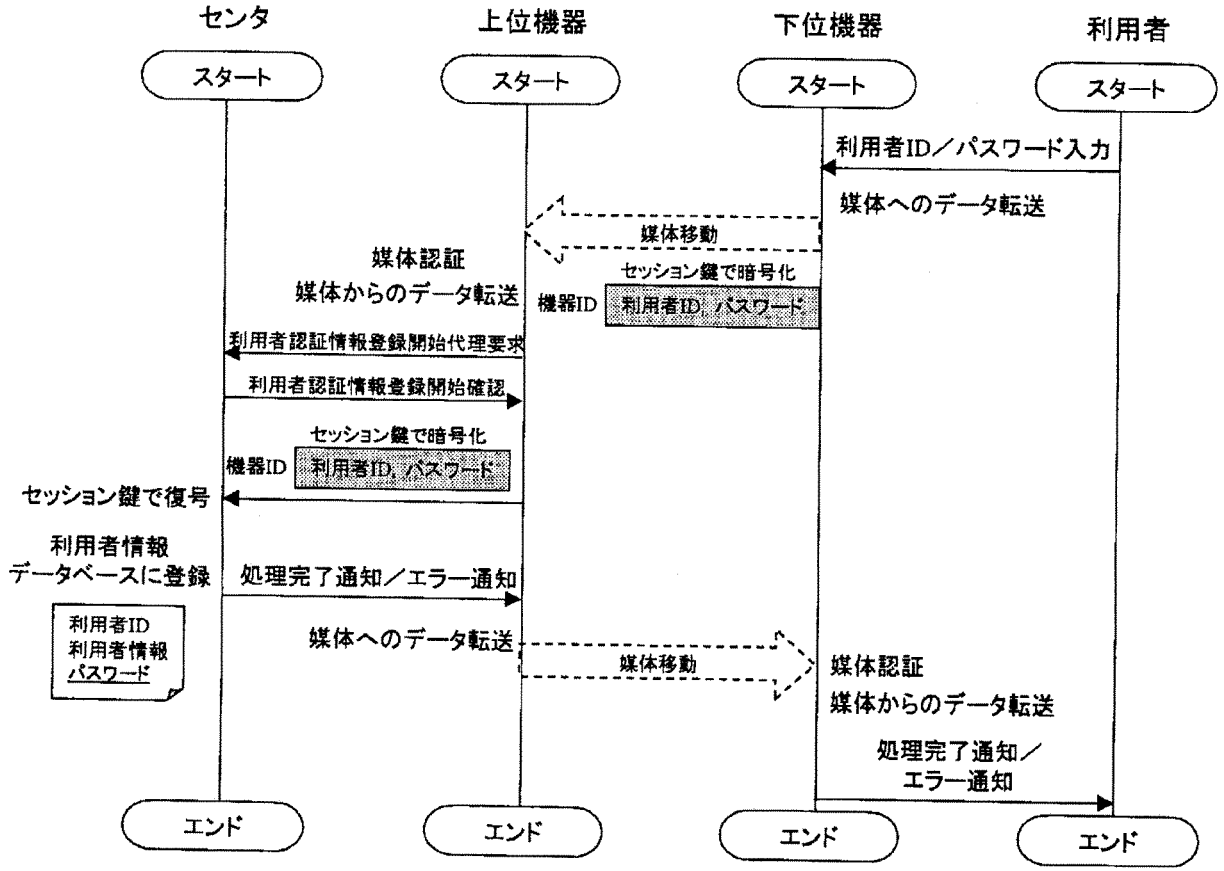


【図３８】

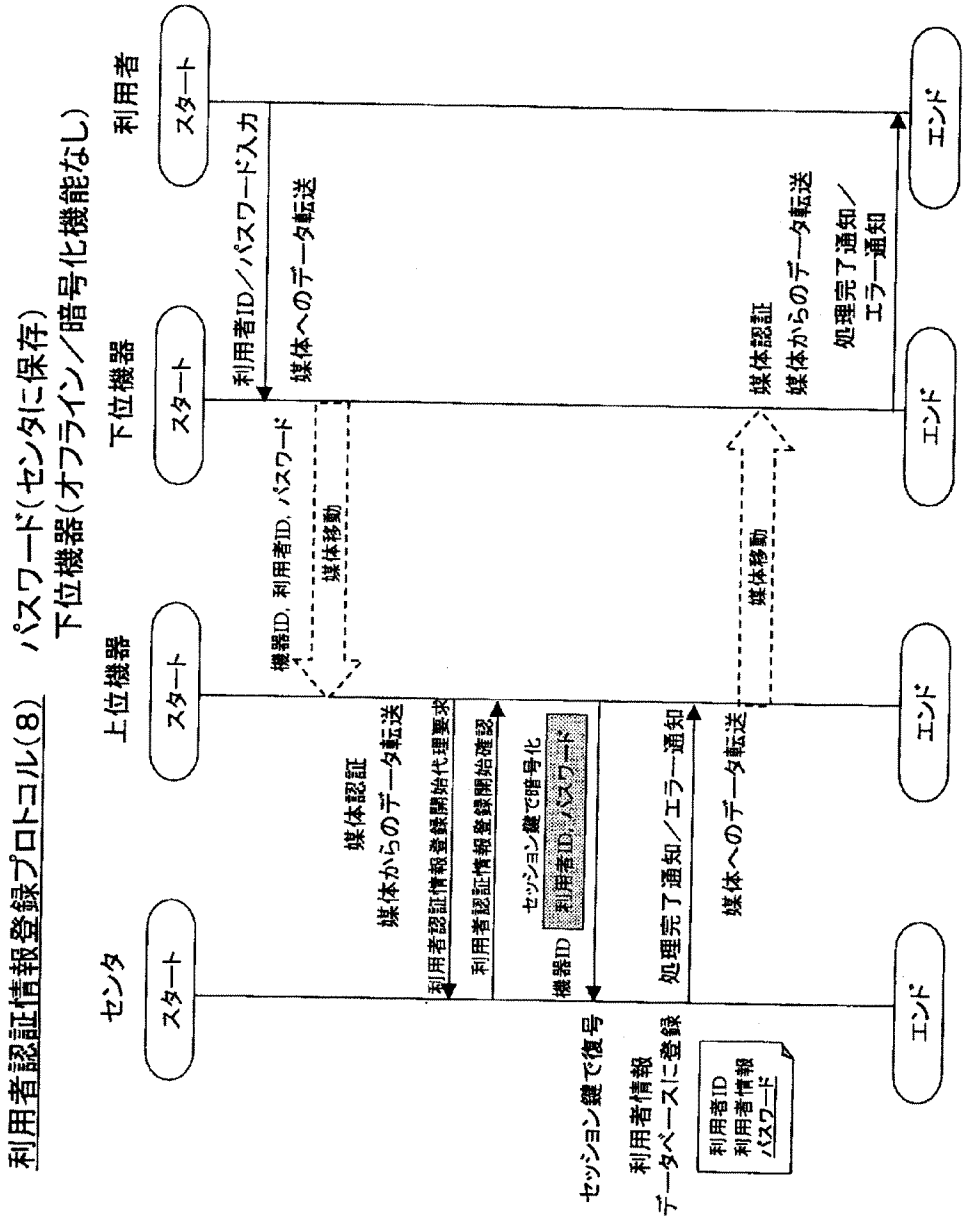

利用者認証情報登録プロトコル(6)　IDカード(センタに保存)
上位機器・下位機器(オンライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
利用者認証情報登録開始要求
利用者認証情報登録開始確認
カードセット
カードからのデータ転送
機器ID, 利用者ID,
利用者認証情報
利用者ID通知
セッション鍵で暗号化
利用者ID,
利用者認証情報
機器ID
処理完了通知／エラー通知
エンド
セッション鍵で復号
利用者情報
データベースに登録
利用者ID
利用者情報
機器ID
パスワード

【図３９】

利用者認証情報登録プロトコル(7)　パスワード(センタに保存)　下位機器(オフライン)

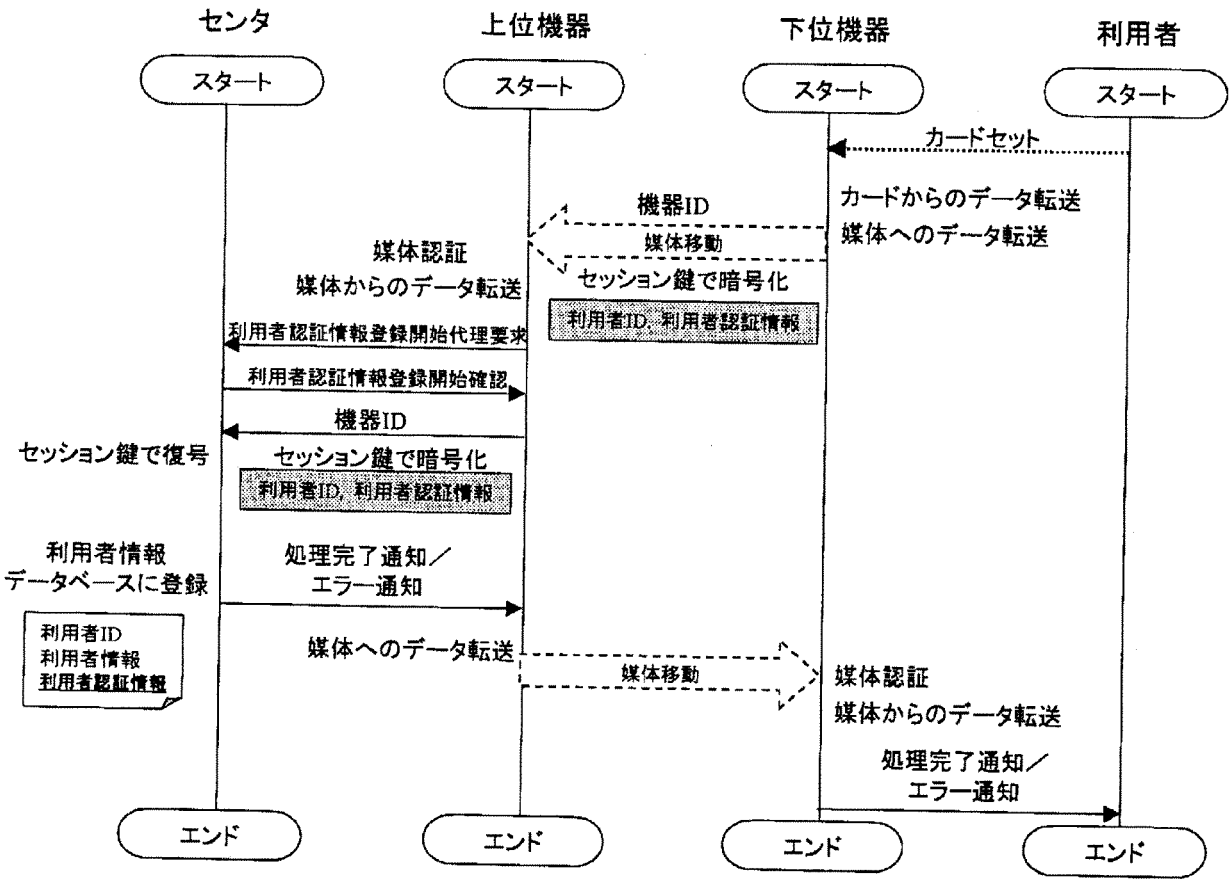


【図４０】

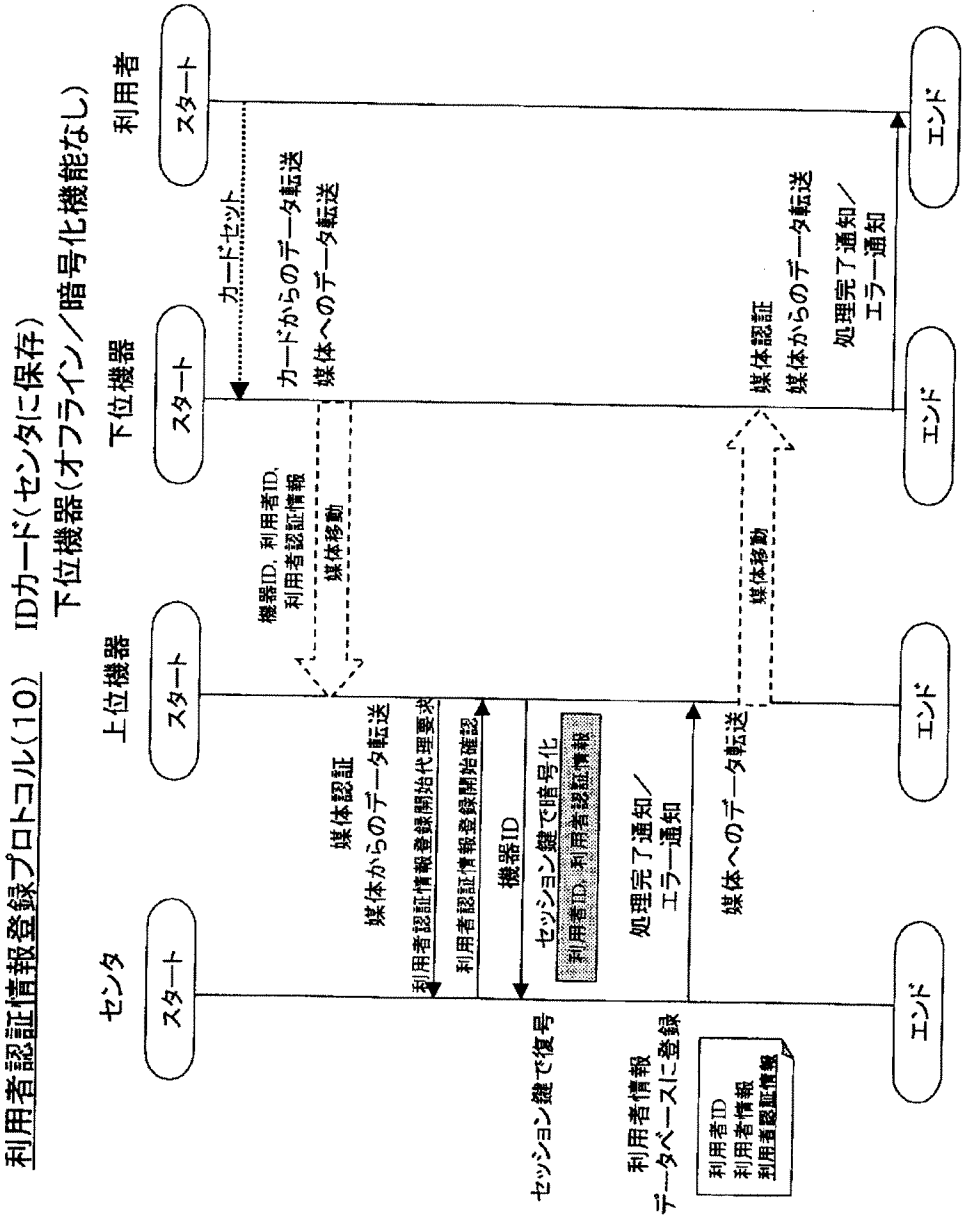

利用者認証情報登録プロトコル(8)　パスワード(センタに保存)
下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
利用者ID／パスワード入力
媒体へのデータ転送
機器ID, 利用者ID, パスワード
媒体移動
媒体認証
媒体からのデータ転送
利用者認証情報登録開始代理要求
利用者認証情報登録開始確認
セッション鍵で暗号化
機器ID
利用者ID, パスワード
セッション鍵で復号
利用者情報
データベースに登録
処理完了通知／エラー通知
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
処理完了通知／
エラー通知
利用者ID
利用者情報
パスワード
エンド
エンド
エンド
エンド

【図４１】

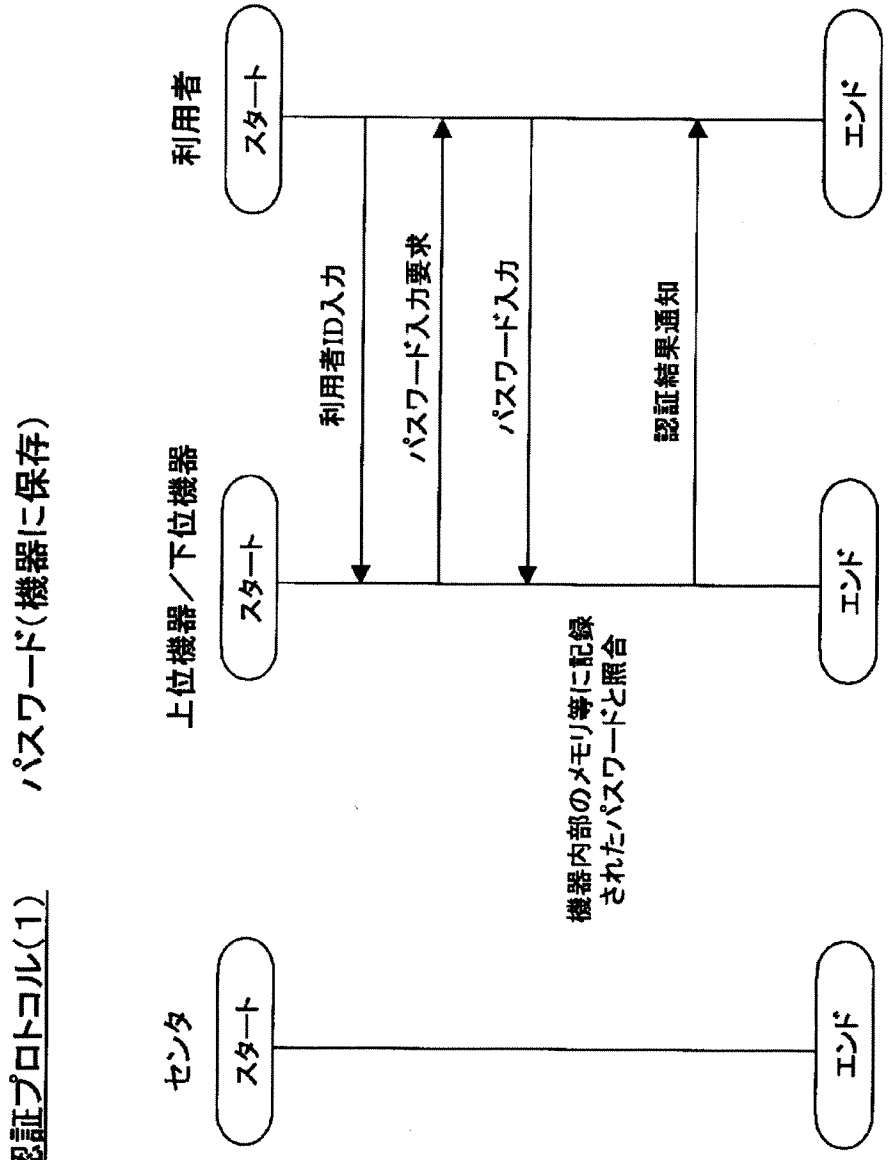
利用者認証情報登録プロトコル(9)　IDカード(センタに保存)　下位機器(オフライン)



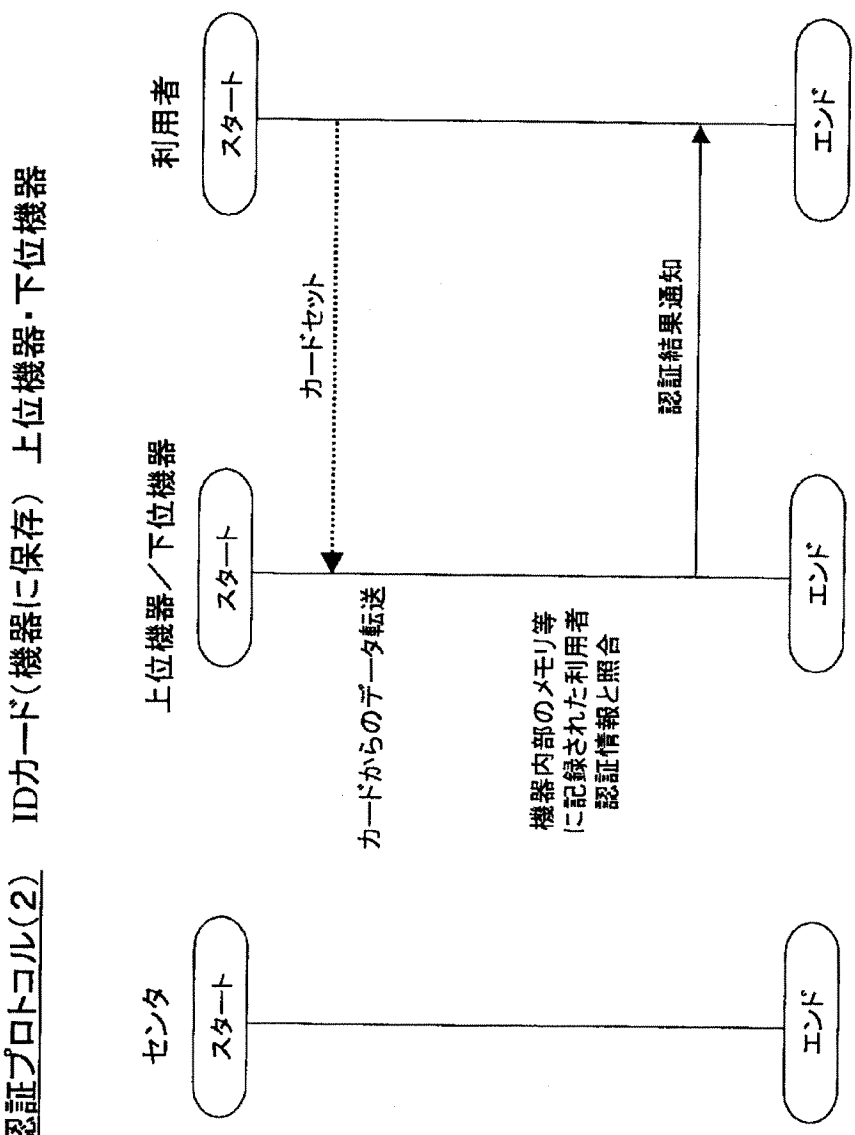
【図４２】


利用者認証情報登録プロトコル(10)　IDカード(センタに保存)
下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
カードセット
機器ID, 利用者ID,
利用者認証情報
媒体移動
カードからのデータ転送
媒体へのデータ転送
媒体認証
媒体からのデータ転送
利用者認証情報登録開始代理要求
利用者認証情報登録開始確認
機器ID
セッション鍵で暗号化
利用者ID, 利用者認証情報
セッション鍵で復号
処理完了通知／
エラー通知
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
処理完了通知／
エラー通知
利用者情報
データベースに登録
利用者ID
利用者情報
利用者認証情報
エンド
エンド
エンド
エンド

【図４３】

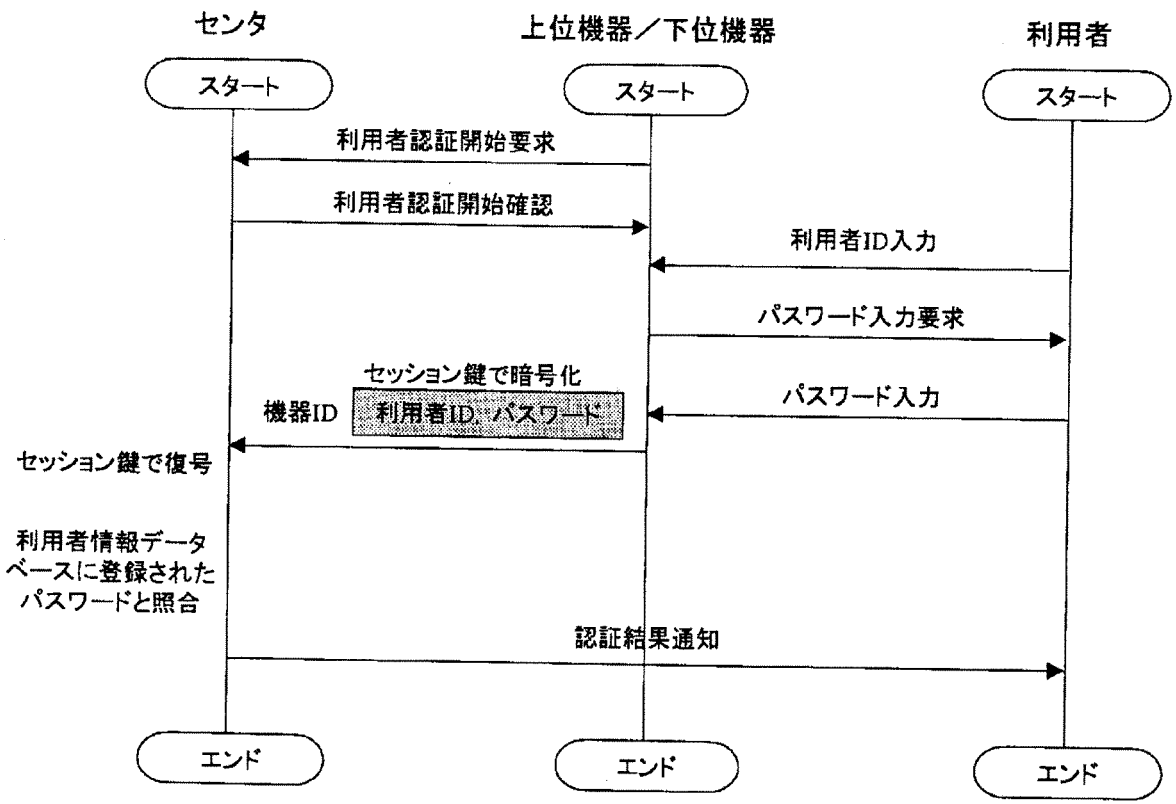

利用者認証プロトコル(1)　パスワード(機器に保存)
センタ
上位機器／下位機器
利用者
スタート
スタート
スタート
利用者ID入力
パスワード入力要求
パスワード入力
認証結果通知
機器内部のメモリ等に記録
されたパスワードと照合
エンド
エンド
エンド

【図４４】

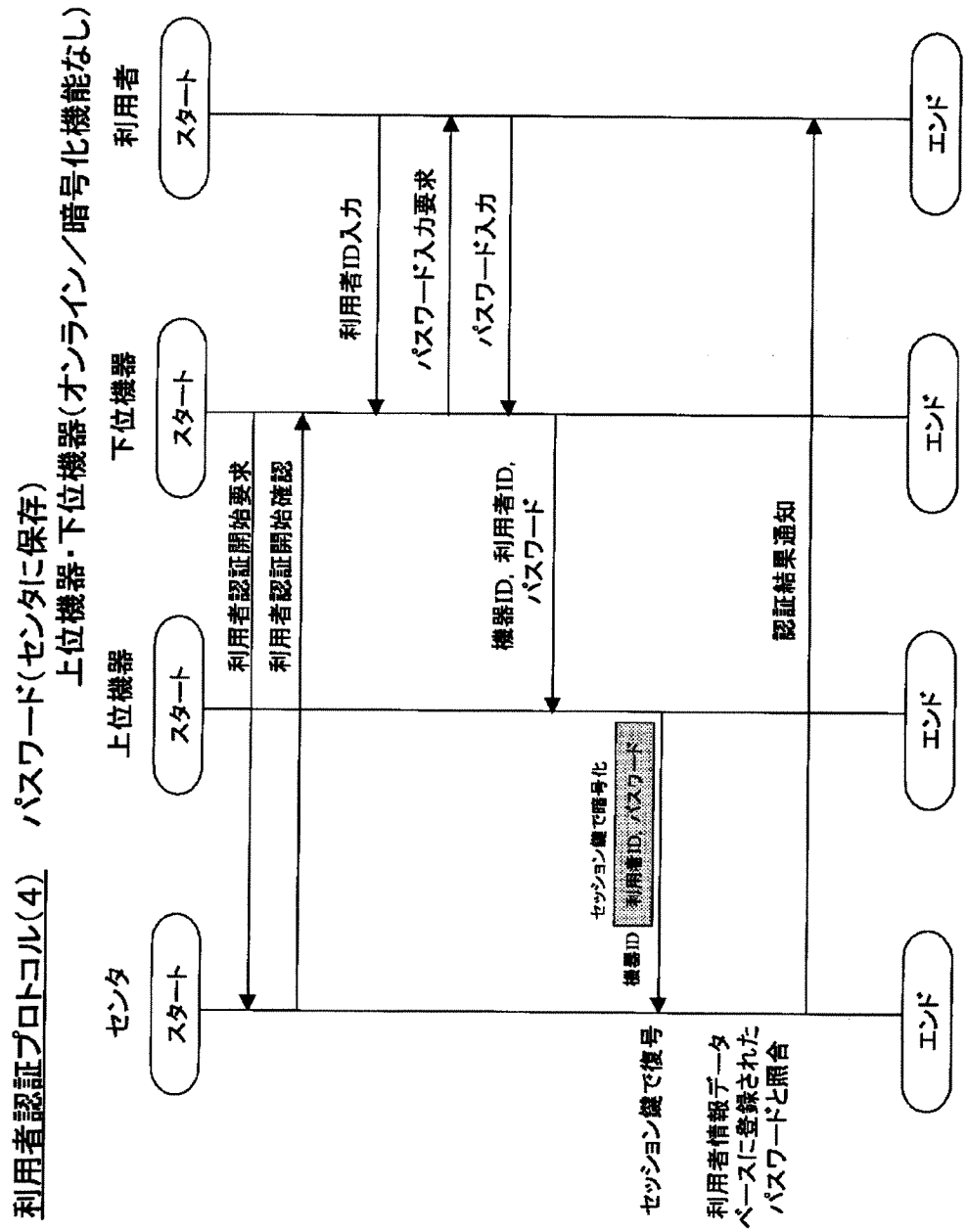

利用者認証プロトコル(2)　IDカード(機器に保存)　上位機器・下位機器
センタ
スタート
エンド
上位機器／下位機器
スタート
エンド
利用者
スタート
エンド
カードセット
カードからのデータ転送
機器内部のメモリ等に記録された利用者認証情報と照合
認証結果通知

【図45】

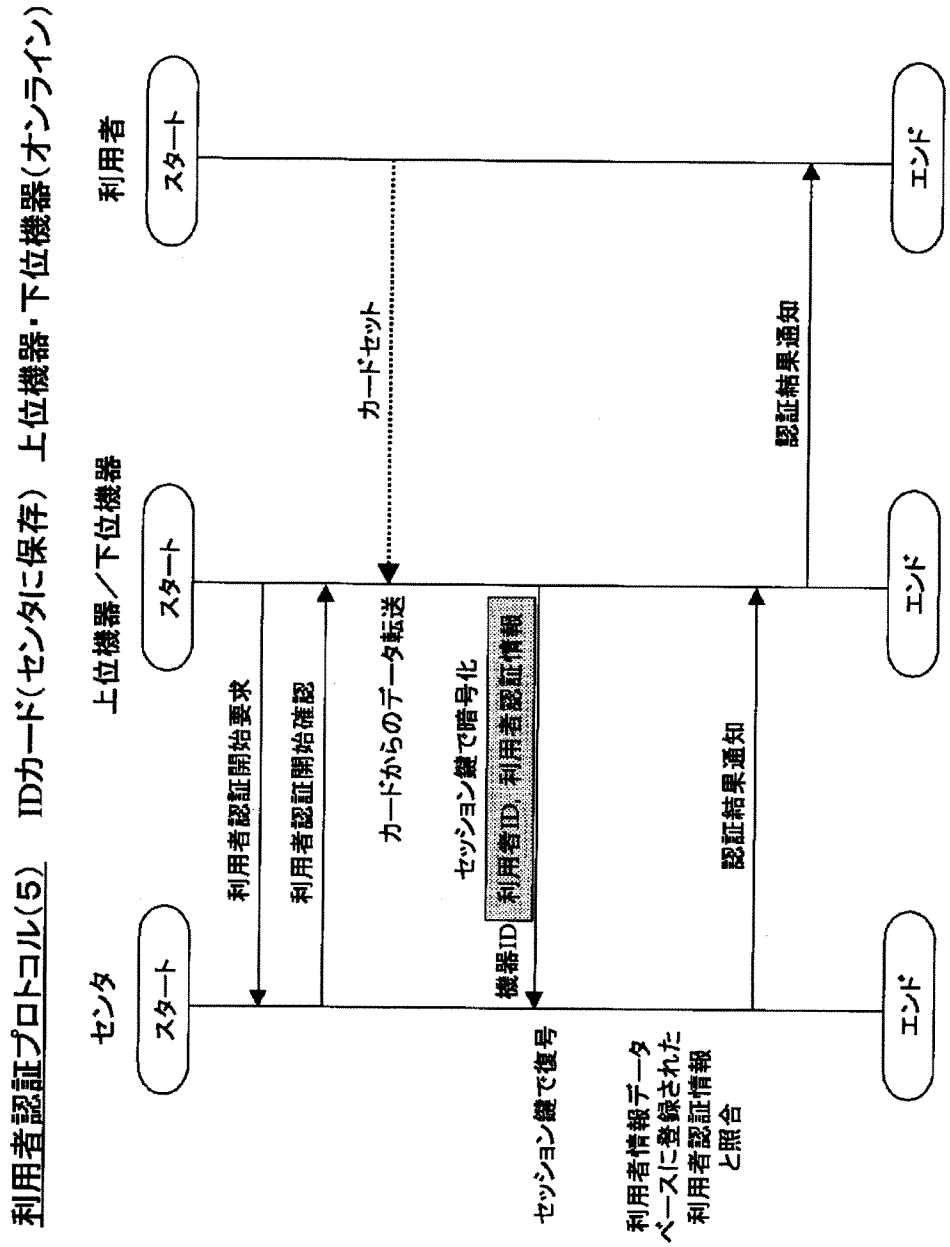
利用者認証プロトコル(3)　パスワード(センタに保存)　上位機器・下位機器(オンライン)



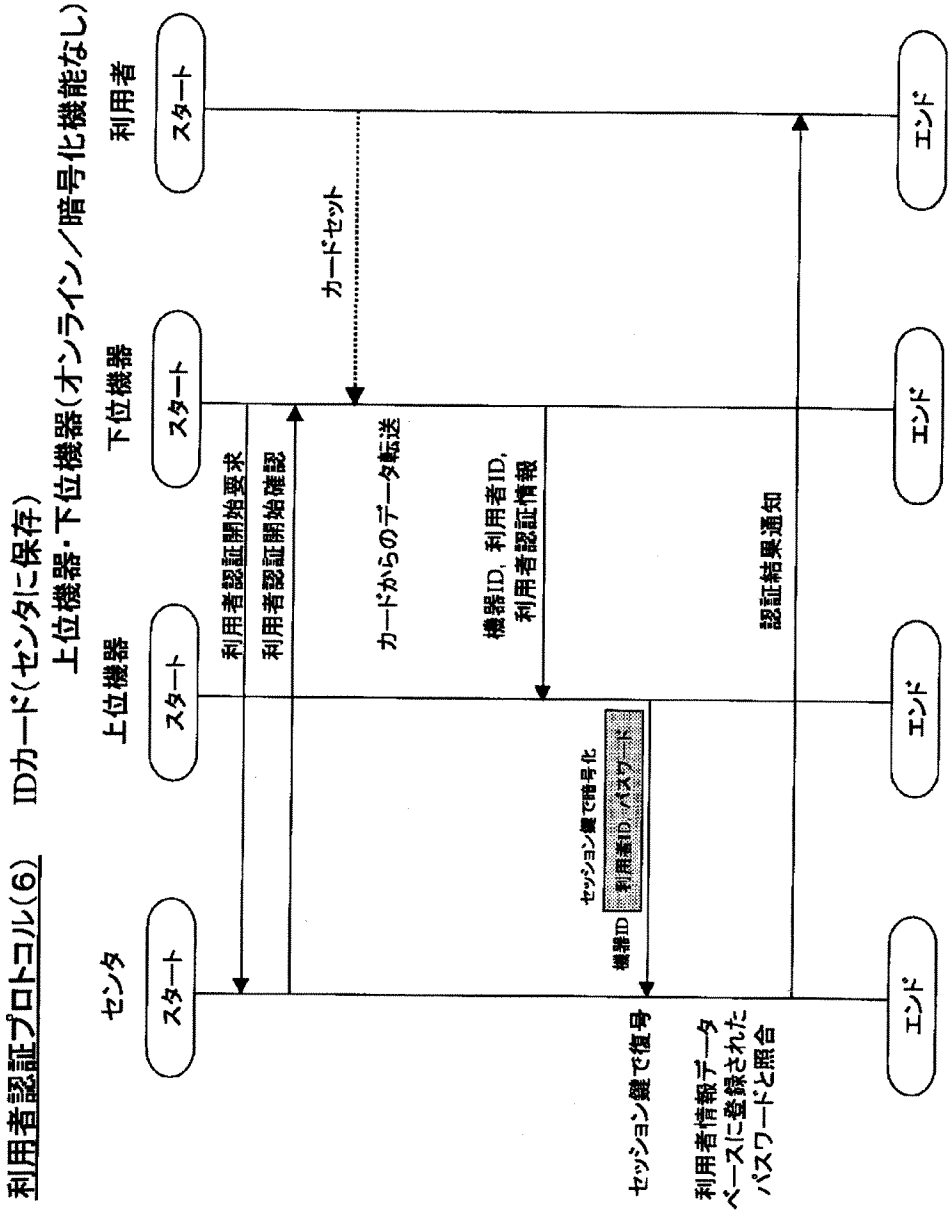
【図４６】


利用者認証プロトコル(4)　パスワード(センタに保存)
上位機器・下位機器(オンライン/暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
利用者認証開始要求
利用者認証開始確認
利用者ID入力
パスワード入力要求
パスワード入力
機器ID, 利用者ID, パスワード
セッション鍵で暗号化
機器ID
利用者ID, パスワード
認証結果通知
エンド
セッション鍵で復号
利用者情報データベースに登録されたパスワードと照合

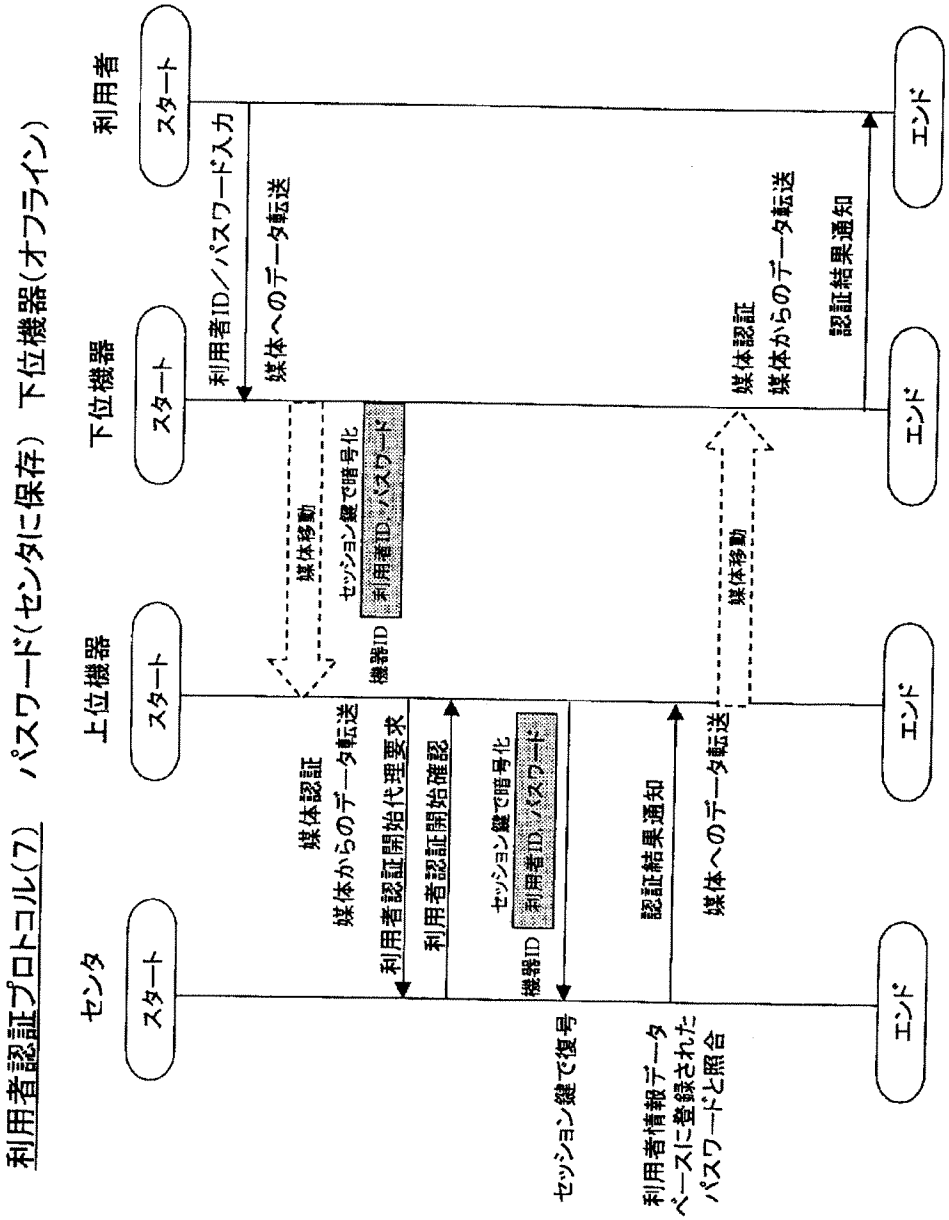
【図４７】


利用者認証プロトコル(5)　IDカード(センタに保存)　上位機器・下位機器(オンライン)
センタ
上位機器／下位機器
利用者
スタート
スタート
スタート
利用者認証開始要求
利用者認証開始確認
カードセット
カードからのデータ転送
セッション鍵で暗号化
機器ID
利用者ID
利用者認証情報
セッション鍵で復号
利用者情報データベースに登録された利用者認証情報と照合
認証結果通知
認証結果通知
エンド
エンド
エンド

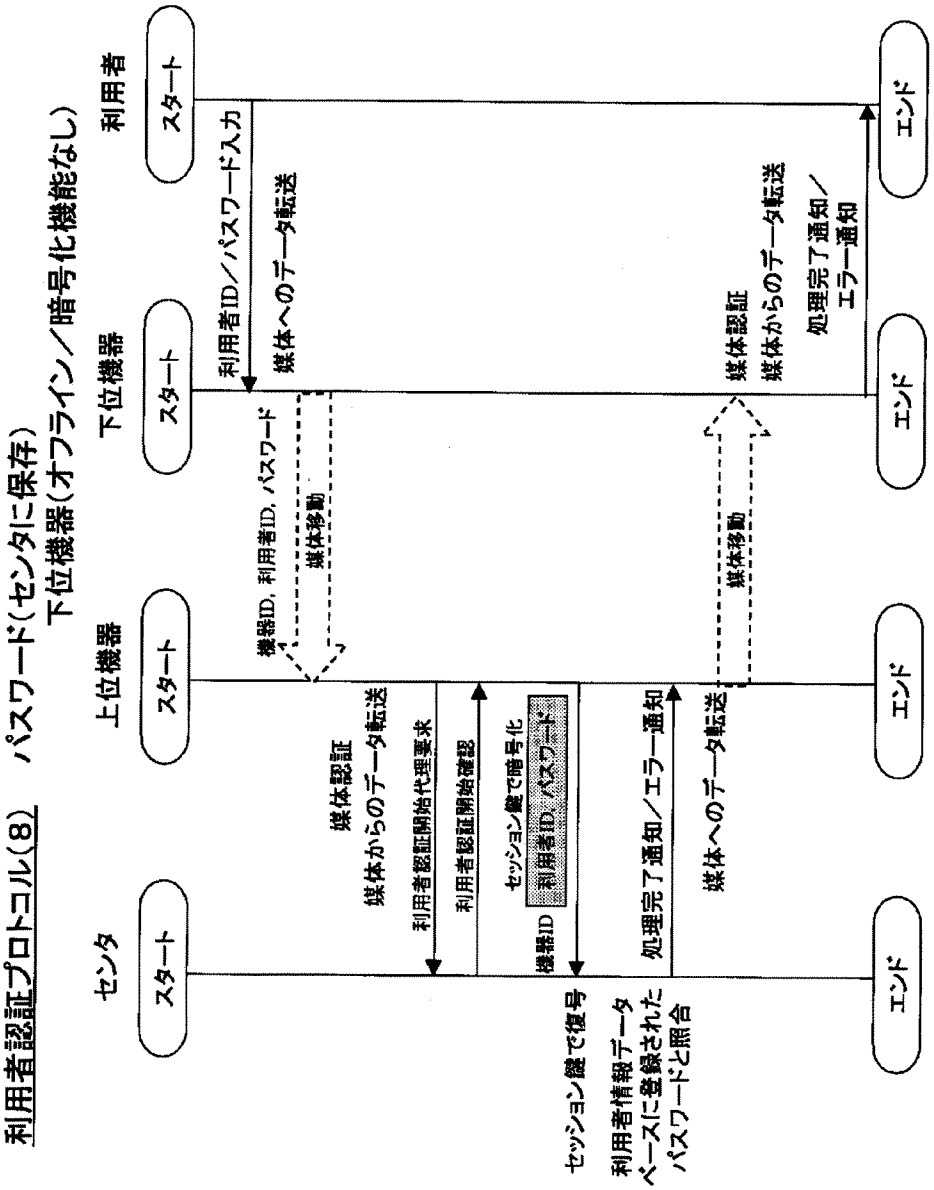
【図４８】


利用者認証プロトコル(6)　IDカード(センタに保存)
上位機器・下位機器(オンライン/暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
利用者認証開始要求
利用者認証開始確認
カードセット
カードからのデータ転送
機器ID, 利用者ID,
利用者認証情報
セッション鍵で暗号化
機器ID
利用者ID, パスワード
認証結果通知
エンド
エンド
エンド
エンド
セッション鍵で復号
利用者情報データ
ベースに登録された
パスワードと照合

【図４９】

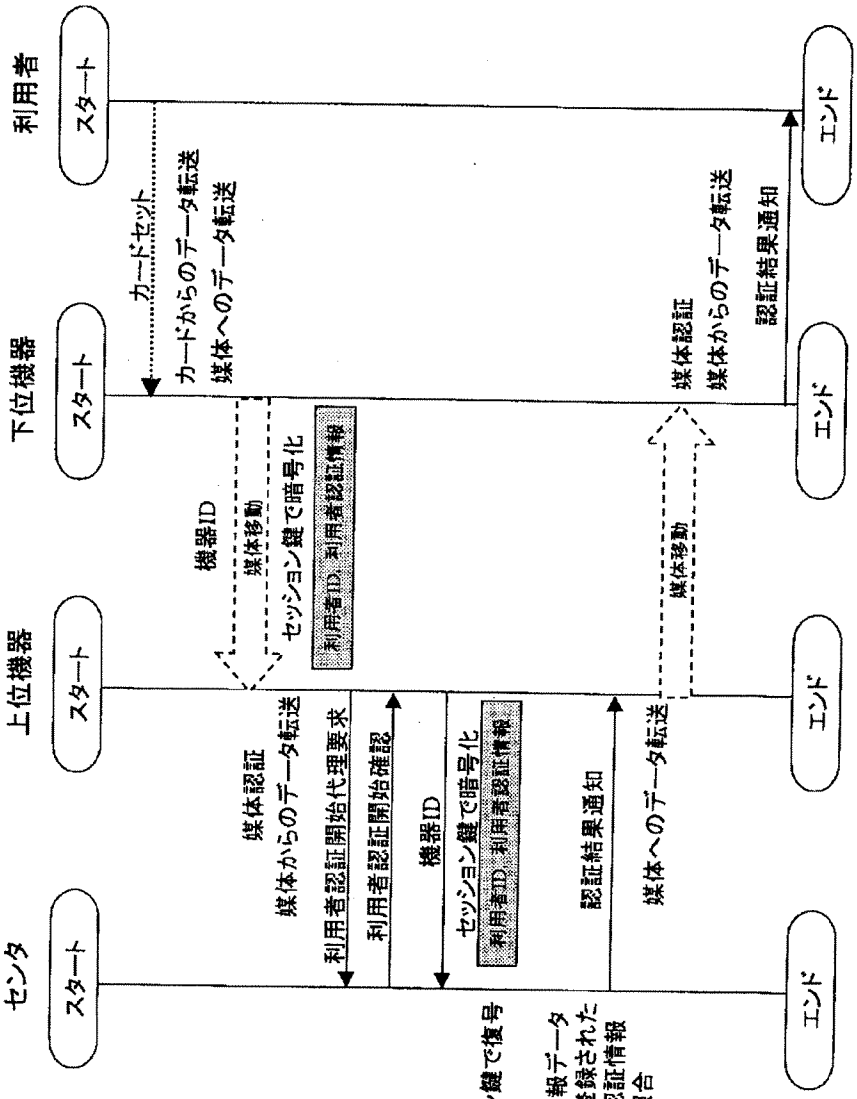

利用者認証プロトコル(7)　パスワード(センタに保存)　下位機器(オフライン)
センタ
上位機器
下位機器
利用者
スタート
利用者ID／パスワード入力
媒体へのデータ転送
媒体移動
セッション鍵で暗号化
利用者ID・パスワード
機器ID
媒体認証
媒体からのデータ転送
利用者認証開始代理要求
利用者認証開始確認
セッション鍵で暗号化
利用者ID・パスワード
機器ID
セッション鍵で復号
利用者情報データベースに登録されたパスワードと照合
認証結果通知
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
認証結果通知
エンド

【図５０】

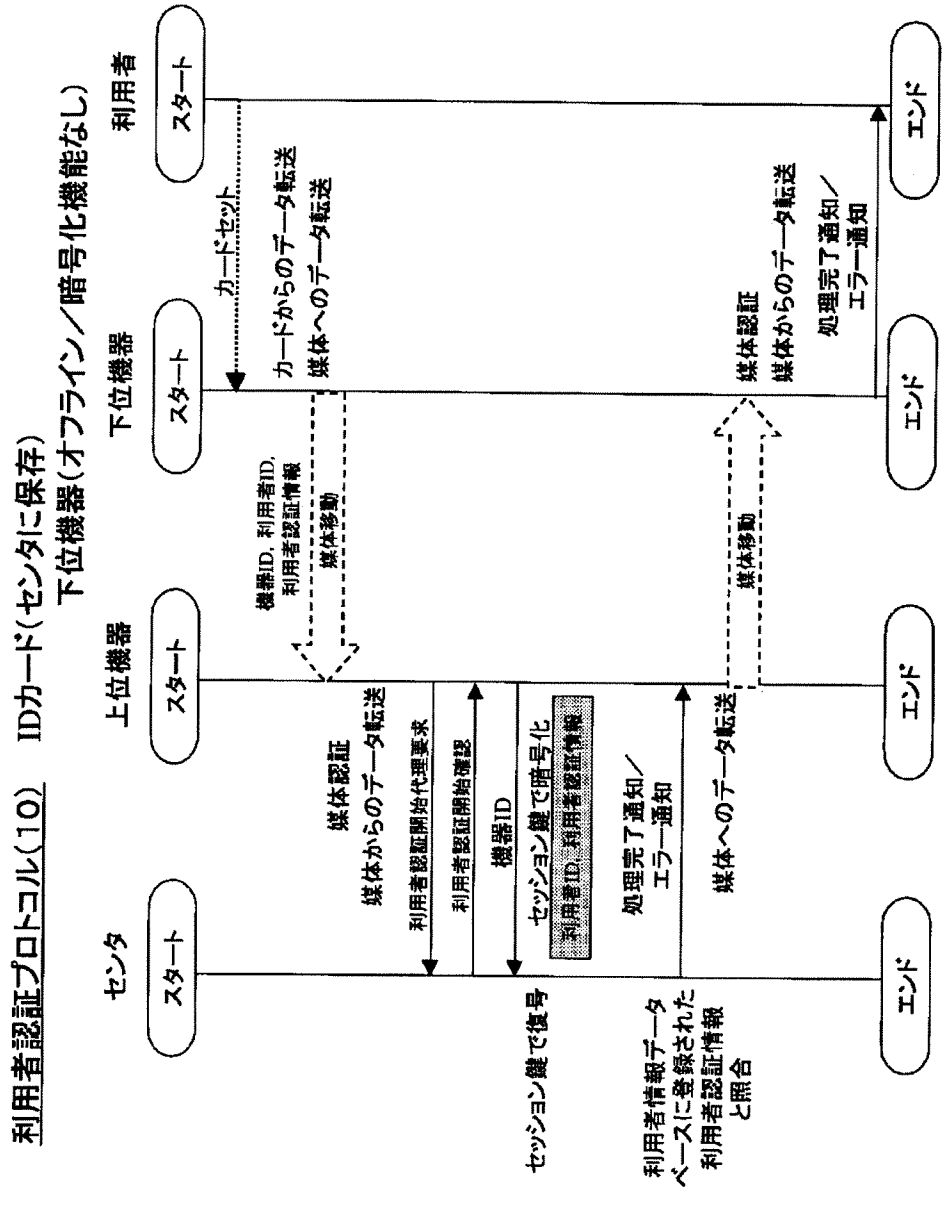

利用者認証プロトコル(8)　パスワード(センタに保存)
下位機器(オフライン/暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
利用者ID/パスワード入力
媒体へのデータ転送
機器ID, 利用者ID, パスワード
媒体移動
媒体認証
媒体からのデータ転送
利用者認証開始代理要求
利用者認証開始確認
セッション鍵で暗号化
機器ID
利用者ID, パスワード
セッション鍵で復号
利用者情報データベースに登録されたパスワードと照合
処理完了通知/エラー通知
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
処理完了通知/
エラー通知
エンド
エンド
エンド
エンド

【図５１】

利用者認証プロトコル(9)　IDカード(センタに保存)　下位機器(オフライン)

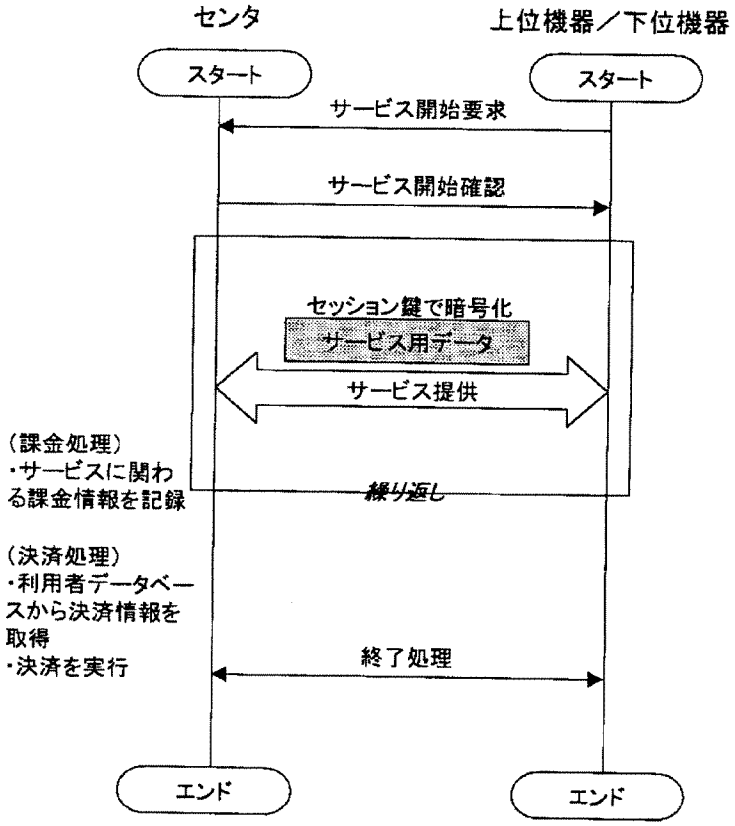


【図５２】


利用者認証プロトコル(10)　IDカード(センタに保存)
下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
利用者
スタート
スタート
スタート
スタート
カードセット
機器ID，利用者ID，
利用者認証情報
媒体移動
カードからのデータ転送
媒体へのデータ転送
媒体認証
媒体からのデータ転送
処理完了通知／
エラー通知
エンド
エンド
エンド
エンド
媒体認証
媒体からのデータ転送
利用者認証開始代理要求
利用者認証開始確認
機器ID
セッション鍵で暗号化
利用者ID，利用者認証情報
媒体へのデータ転送
媒体移動
処理完了通知／
エラー通知
セッション鍵で復号
利用者情報データ
ベースに登録された
利用者認証情報
と照合

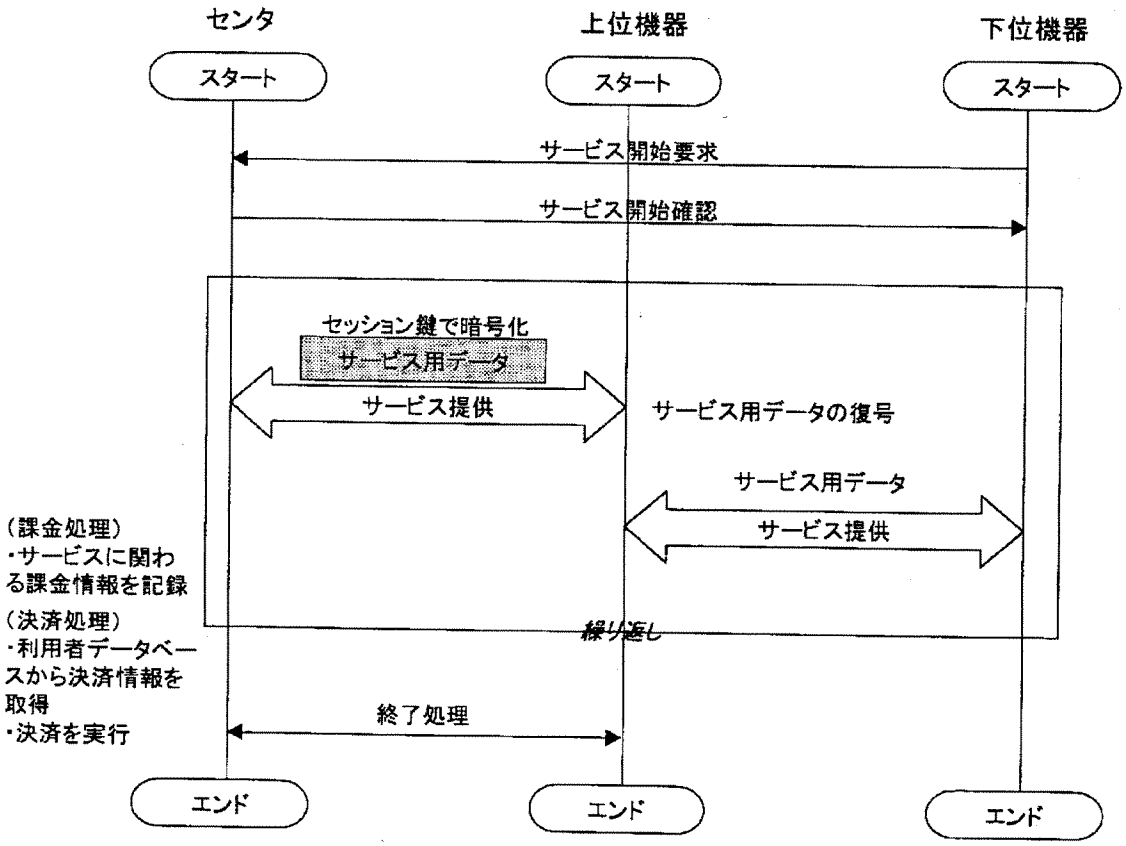
【図５３】

サービスプロトコル(１)　　上位機器，下位機器(オンライン)

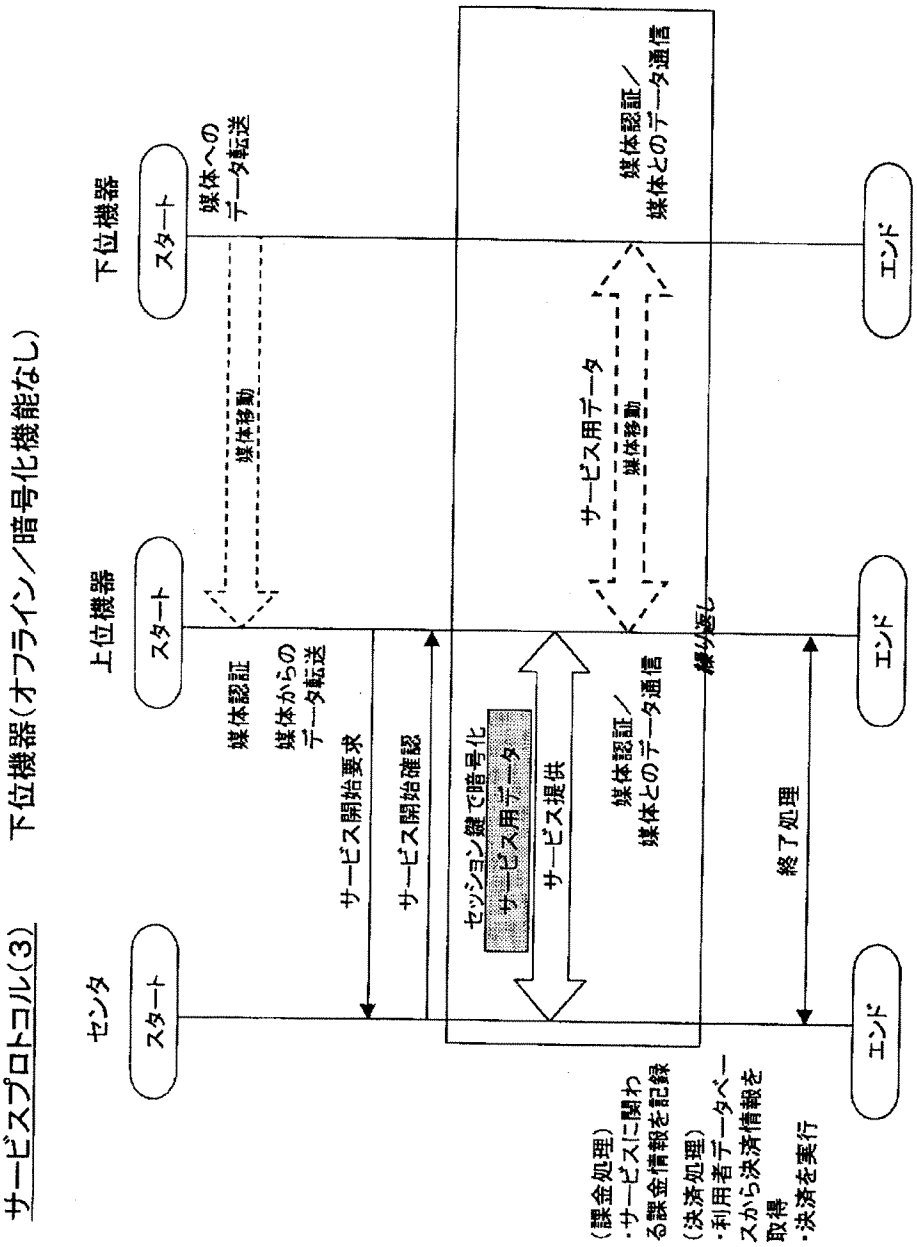


【図５４】

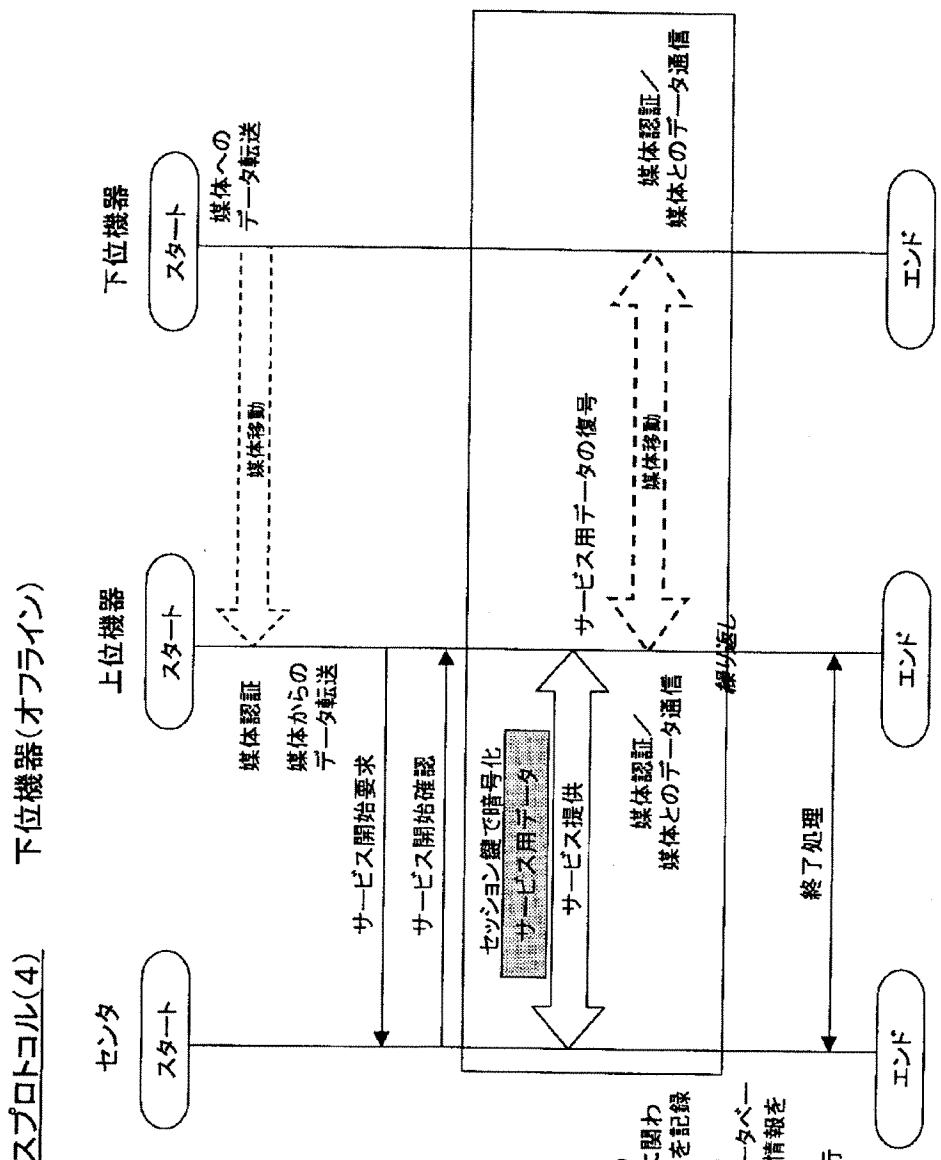
サービスプロトコル(2)　　上位機器，下位機器(オンライン／暗号化機能なし)



【図５５】

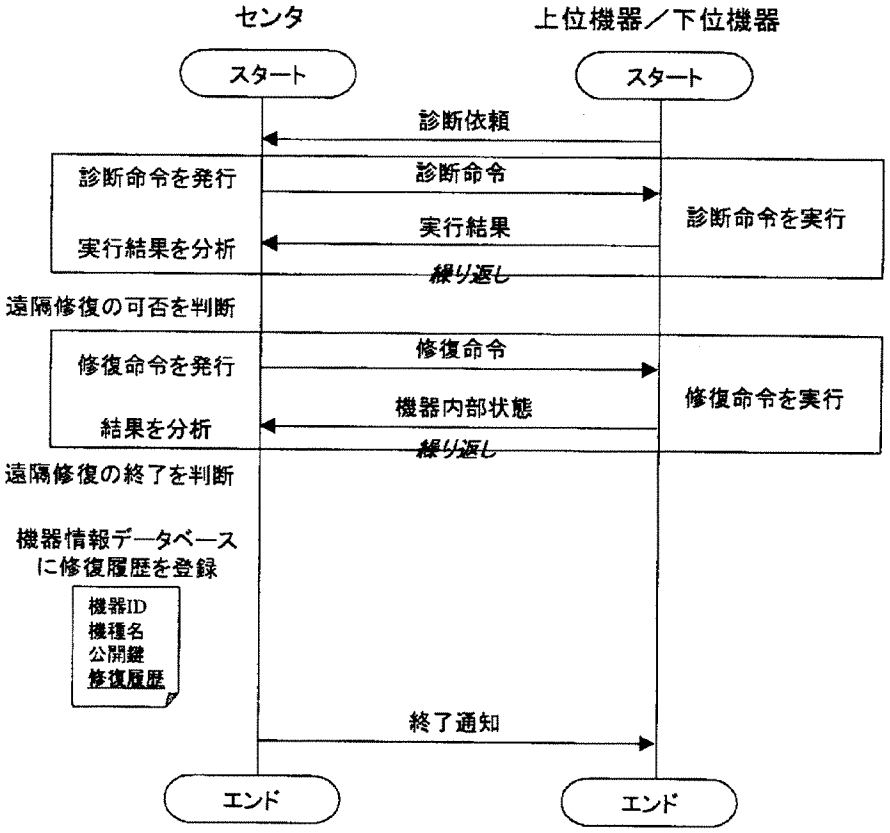

サービスプロトコル(3)　下位機器(オフライン／暗号化機能なし)
センタ
上位機器
下位機器
スタート
スタート
スタート
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
サービス開始要求
サービス開始確認
セッション鍵で暗号化
サービス用データ
サービス提供
媒体認証／媒体とのデータ通信
サービス用データ
媒体移動
媒体認証／媒体とのデータ通信
繰り返し
エンド
エンド
エンド
終了処理
(課金処理)
・サービスに関わる課金情報を記録
(決済処理)
・利用者データベースから決済情報を取得
・決済を実行

【図５６】


サービスプロトコル(4)　下位機器(オフライン)
センタ
上位機器
下位機器
スタート
スタート
スタート
媒体へのデータ転送
媒体移動
媒体認証
媒体からのデータ転送
サービス開始要求
サービス開始確認
セッション鍵で暗号化
サービス用データ
サービス提供
サービス用データの復号
媒体移動
媒体認証／媒体とのデータ通信
媒体認証／媒体とのデータ通信
繰り返し
終了処理
エンド
エンド
エンド
(課金処理)
・サービスに関わる課金情報を記録
(決済処理)
・利用者データベースから決済情報を取得
・決済を実行

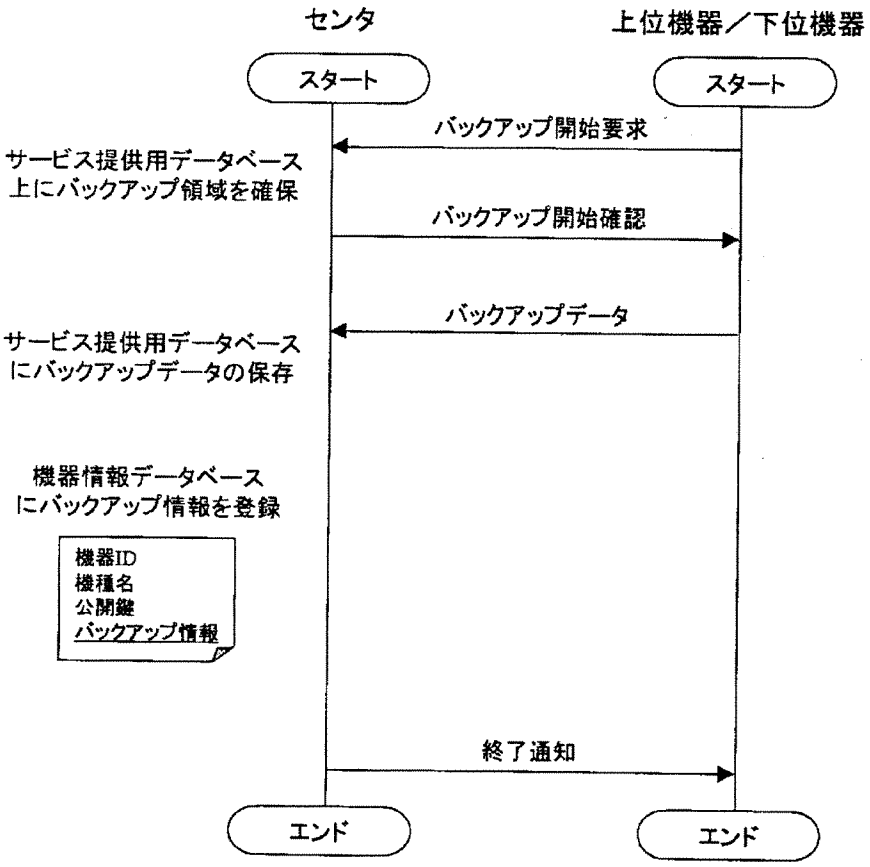
【図５７】

遠隔診断・修復


センタ
上位機器／下位機器
スタート
スタート
診断依頼
診断命令を発行
診断命令
診断命令を実行
実行結果
実行結果を分析
繰り返し
遠隔修復の可否を判断
修復命令を発行
修復命令
修復命令を実行
機器内部状態
結果を分析
繰り返し
遠隔修復の終了を判断
機器情報データベースに修復履歴を登録
機器ID
機種名
公開鍵
修復履歴
終了通知
エンド
エンド

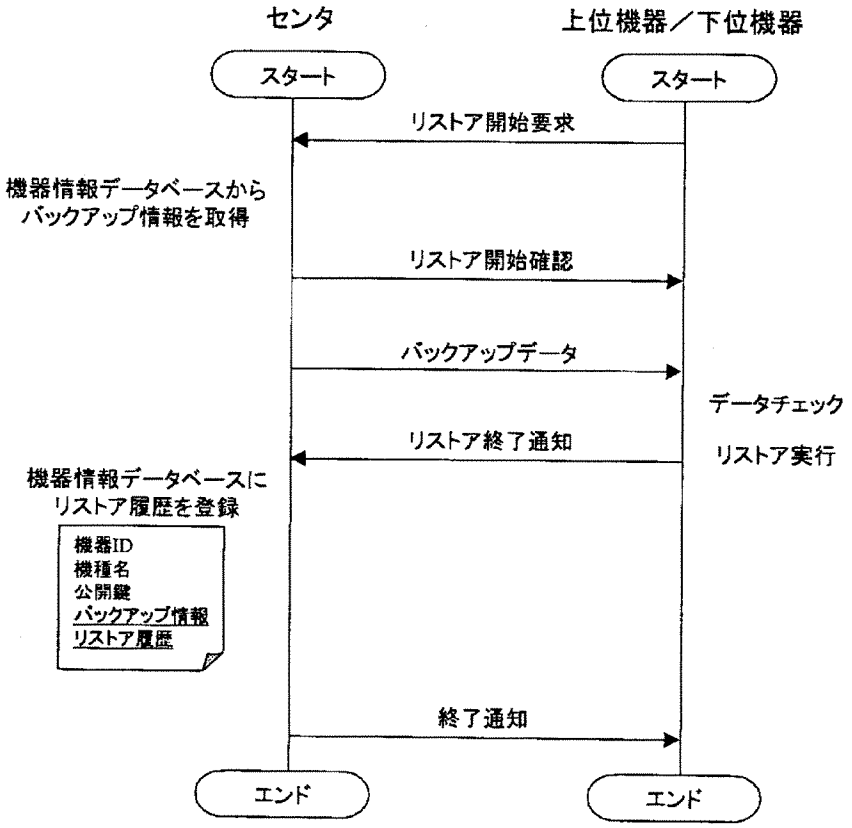
【図５８】

バックアップ


センタ
上位機器／下位機器
スタート
スタート
バックアップ開始要求
サービス提供用データベース
上にバックアップ領域を確保
バックアップ開始確認
バックアップデータ
サービス提供用データベース
にバックアップデータの保存
機器情報データベース
にバックアップ情報を登録
機器ID
機種名
公開鍵
バックアップ情報
終了通知
エンド
エンド

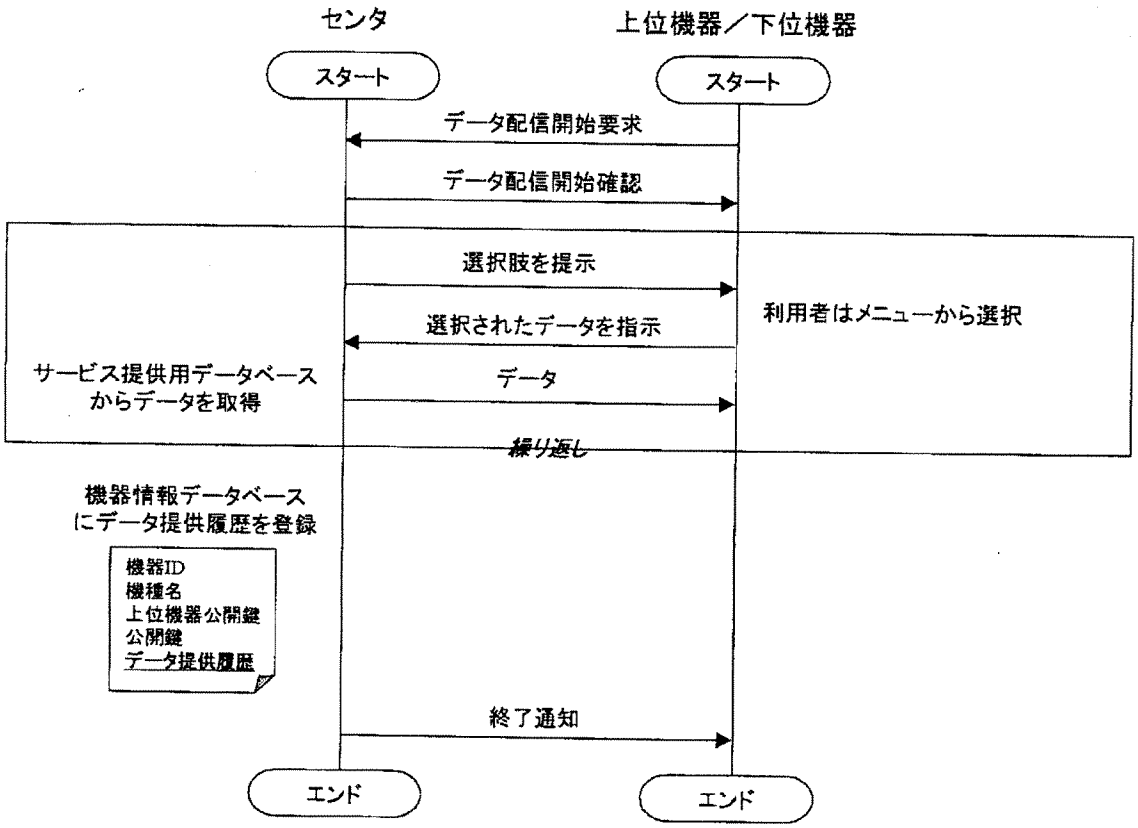
【図５９】

リストア


センタ
上位機器／下位機器
スタート
スタート
リストア開始要求
機器情報データベースから
バックアップ情報を取得
リストア開始確認
バックアップデータ
データチェック
リストア終了通知
リストア実行
機器情報データベースに
リストア履歴を登録
機器ID
機種名
公開鍵
バックアップ情報
リストア履歴
終了通知
エンド
エンド

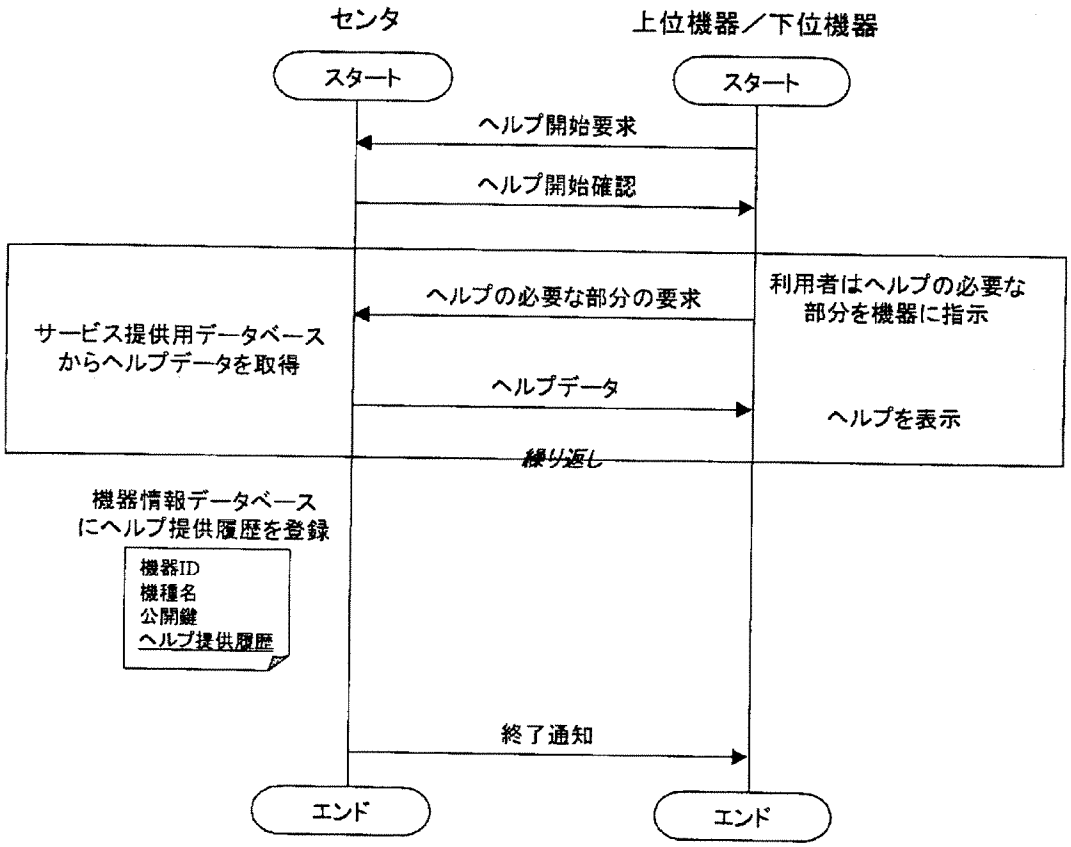
【図６０】

データ配信

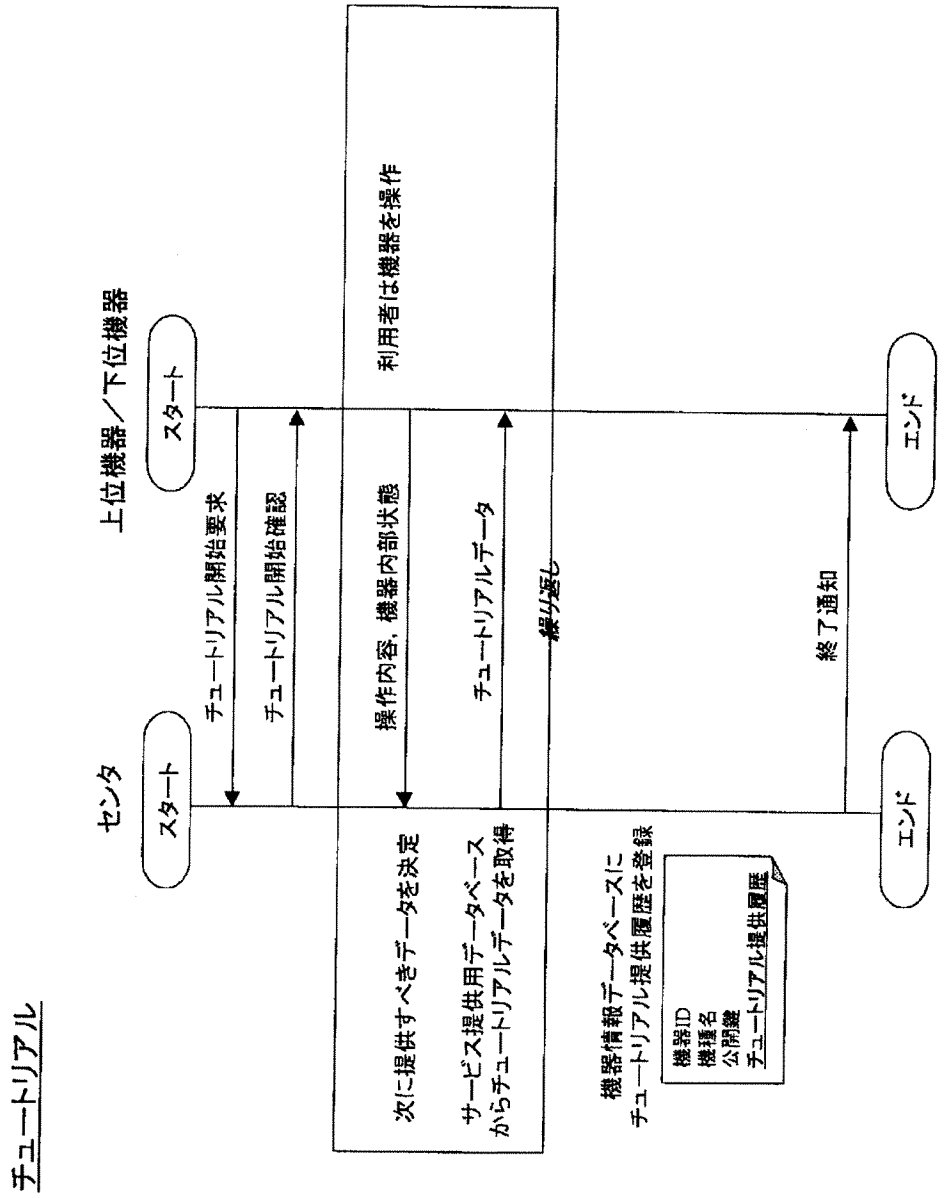

センタ
上位機器／下位機器
スタート
スタート
データ配信開始要求
データ配信開始確認
選択肢を提示
利用者はメニューから選択
選択されたデータを指示
サービス提供用データベース
からデータを取得
データ
繰り返し
機器情報データベース
にデータ提供履歴を登録
機器ID
機種名
上位機器公開鍵
公開鍵
データ提供履歴
終了通知
エンド
エンド

【図６１】

ヘルプ


センタ
上位機器／下位機器
スタート
スタート
ヘルプ開始要求
ヘルプ開始確認
ヘルプの必要な部分の要求
利用者はヘルプの必要な部分を機器に指示
サービス提供用データベースからヘルプデータを取得
ヘルプデータ
ヘルプを表示
繰り返し
機器情報データベースにヘルプ提供履歴を登録
機器ID
機種名
公開鍵
ヘルプ提供履歴
終了通知
エンド
エンド

【図６２】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)	
G06F	17/60	176	G06F	17/60	176A	5K067
H04Q	7/38		H04B	7/26	109R	9A001
H04L	9/32		H04L	9/00	673B	
	12/66			11/20	B	

(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B049 AA05 BB00 BB46 CC03 CC22 CC36 CC39 CC48 DD04 EE03 EE05 EE23 EE56 GG04 GG07 GG10
5B085 AE23
5B089 HA01 HA06 HA11 JB14 JB19 KA12 KA17 KB13 KC58 KG03 KH30
5J104 AA07 KA02 KA04 KA05 NA03
5K030 GA15 HA05 HB08 HC01 HC14 HD01 HD06 JT09 LD20
5K067 AA30 BB04 DD17 EE02 EE16 HH11 HH24 HH36
9A001 CC03 CZ05 EE03 JJ01 JJ25 LL03